On The Security of Wide Area Measurement System and Phasor Data Collection

Reem Kateb

A Thesis

In

The Concordia Institute

for

Information Systems Engineering

Presented in Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy (Information and Systems Engineering) at

Concordia University

Montréal, Québec, Canada

January 2019

© Reem Kateb, 2019

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: Reem Kateb

Entitled: On The Security of Wide Area Measurement System and Phasor Data Collection

and submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy (Information and Systems Engineering)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Abdel R. Sebak

_____ External Examiner
Dr. Mohamed IbnKahla

_____ External to program
Dr. Anjali Agarwal

_____ Examiner
Dr. Roch Glitho

_____ Examiner
Dr. Amr Youssef

_____ Thesis Co-Supervisor
Dr. Chadi Assi

_____ Thesis Co-Supervisor
Dr. Mourad Debbabi

Approved by _____
Dr. Chadi Assi, Graduate Program Director

March 4, 2019

_____
Dr. Amir Asif, Dean
Gina Cody School of Engineering & Computer Science

Abstract

On The Security of Wide Area Measurement System and Phasor Data Collection

Reem Kateb, Ph.D.

Concordia University, 2019

Smart grid is a typical cyber-physical system that presents the dependence of power system operations on cyber infrastructure for control, monitoring, and protection purposes. The rapid deployment of phasor measurements in smart grid transmission system has opened opportunities to utilize new applications and enhance the grid operations. Thus, the smart grid has become more dependent on communication and information technologies such as Wide Area Measurement Systems (WAMS). WAMS are used to collect real-time measurements from different sensors such as Phasor Measurement Units (PMUs) installed across widely dispersed areas. Such system will improve real-time monitoring and control; however, recent studies have pointed out that the use of WAMS introduces significant vulnerabilities to cyber-attacks that can be leveraged by attackers. Therefore, preventing or reducing the damage of cyber attacks on WAMS is critical to the security of the smart grid. In this thesis, we focus our attention on the relation between WAMS security and the IP routing protocol, which is an essential aspect to the collection of sensors measurements.

Synchrophasor measurements from different PMUs are transferred through a data network and collected at one or multiple data concentrators. The timely collection of phasors

from PMU dispersed across the grid allows to maintain system observability and take corrective actions when needed. This collection is made possible through Phasor Data Concentrators (PDCs) that time-align and aggregate phasor measurements, and forward the resulting stream to be used by monitoring and control applications. WAMS applications relying on these measurements have strict and stringent delay requirements, e.g., end to end delay as well as delay variation between measurements from different PMUs. Measurements arriving past a predetermined time period at a data concentrator will be dropped, causing incompleteness of data and affecting WAMS applications and hence the system's operations. It has been shown that non-functional properties, such as data delay and packet drops, have a negative impact on the system functionality.

We show that simply forwarding measurements from PMUs through shortest routes to phasor data collectors may result in data being dropped at their destinations. We believe therefore that there is a strong interplay between the routing paths (delays along the paths) for gathering the measurements and the value of timeout period. This is particularly troubling when a malicious attacker deliberately causes delays on some communication links along the shortest routes. Therefore, we present a mathematical model for constructing forwarding trees for PMUs' measurements which satisfy the end to end delay as well as the delay variation requirements of WAMS applications at data concentrators. We show that a simple shortest path routing will result in larger fraction of data drop and that our method will find a suitable solution. Then, we study the relation between cyber-attack propagation and IP multicast routing. To this extent, we formulate the problem as the construction of a multicast tree that minimizes the propagation of cyber-attacks while satisfying real-time and capacity requirements. The proposed attack propagation multicast tree is evaluated using different IEEE test systems. Finally, cyber-attacks resulting in the disconnection of PDC(s) from WAMS initiate a loss of its phasor stream and incompleteness in the observability of the power system. Recovery strategies based on the re-routing of lost phasors to

other connected and available PDCs need to be designed while considering the functional requirements of WAMS. We formulate a recovery strategy from loss of compromised or failed PDC(s) in the WAMS network based on the rerouting of disconnected PMUs to functional PDCs. The proposed approach is mathematically formulated as a linear program and tested on standard IEEE test systems. These problems will be extensively studied throughout this thesis.

Acknowledgments

Foremost, I would like to express my sincere gratitude and special appreciation to my supervisors, Professor Chadi Assi and Professor Mourad Debbabi, for their continuous support, patience, motivation, enthusiasm, and immense knowledge. Their guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisors and mentors for my Ph.D studies.

I would like to thank all my collaborators and co-authors for the fruitful discussion and struggles we shared. I must say, I am indebted for all the promising ideas we have come across and struggled with, the one that worked and the ones that did not, they all were a valuable source of knowledge and inspiration.

I am particularly thankful for the fantastic environment at the smart grid security group. It is truly amazing how many exciting discussions and collaborations started during the weekly group meetings.

A special thanks to my family. Words can not express how grateful I am to my parents for all of the sacrifices that they made on my behalf. Your prayer for me was what sustained me thus far. I would also like to thank all of my friends who supported me in writing, and helped me to strive towards my goal. At the end I would like express appreciation to my beloved husband Yousef, who spent sleepless nights with me and was always my support in the moments when there was no one to answer my queries. The last word goes for Aleen and Sarah, my girls, who has been the light of my life and have given me the extra strength and motivation to get things done. This thesis is dedicated to them.

Contents

List of Figures

List of Tables

1. Introduction

1.1 Smart Grid

The current electrical power system is by far the most significant and sophisticated engineering system of the 20*th* century. This system contains a large network that connects centralized generation, transmission, distribution, control centre, and power consumers. Even though the traditional power system has served well in providing power supply to consumers, many of today's electrical grids are operating near to their stability limits due to the increased power demands that have not been accompanied by an increase in transmission capacity. As a result, the stability of such power systems becomes a serious issue since operational security and reliability standards can be violated. Therefore, the grid is becoming increasingly outdated and overburdened, leading to costly blackouts and environmental damages [5]. Recent large blackouts and outages, such as the 2003 North American and the 2015 Ukrainian blackouts, stand as a proof that the current grid lacks automated analysis, have a slow response time, and low situational awareness [5, 6]. Further, recent studies show that 8% of the produced power is wasted along transmission lines [7]. As current power grids do not consist of storage units, the produced energy needs to be adjusted to power consumption [8]. Moreover, to manage, operate, and control the grid in a reliable and safe environment, a series of complex technical tasks at different times and geographic areas must be accomplished.

The occurrence of major blackouts in many power systems around the world has necessitated the use of better system monitoring and control methodologies. Under such challenges, carrying out the grid operations on a real-time basis and responding to contingencies are critical for maintaining a healthy, reliable, and stable power grid. Therefore, an ever-increasing effort has been made in many countries to the development of a more intelligent, responsive, efficient, and environmentally friendly "smarter" power grid, known as smart grid [7]. The main target of such grid is to connect the components of the electrical grid via communication networks, such as Internet or sensor networks, to collect data about the grid's condition and consumers' requirements.

The future smart grid can be defined as the modernization of the current power grid for improved efficiency, reliability, and safety, with a sufficient integration of renewable and alternative energy sources through modern controls and communication technologies [9]. The smart grid enables two-way communication of data and electrical power to provide consumers with information to better manage their power usage. It is self-healing in case of disturbances, such as physical attacks, cyber attacks, or natural disasters. Moreover, its new infrastructure links and utilizes different energy resources, including renewable energy. Additionally, it aims at providing efficient delivery and better power quality [10]. Moreover, the smart grid aims at reducing CO2 emissions. Additionally, a number of Distributed Generators (DG) are inserted in the grid to satisfy the increased electrical demands. Furthermore, original techniques, such as micro-grids that offer electricity for a certain area using one or more DGs are utilized in the new smarter grid. Such grids allow the area to be isolated or connected to the main grid based on the current grid's status, which protects the grid in case of blackouts or disturbances by assisting the self-healing properties of the grid.

The National Institute of Standards and Technology (NIST) proposed a conceptual architecture of the smart grid (Figure (1.1)), along with its electrical and communication flows. The model consists of seven domains: Bulk Generation, Transmission, Distribution,

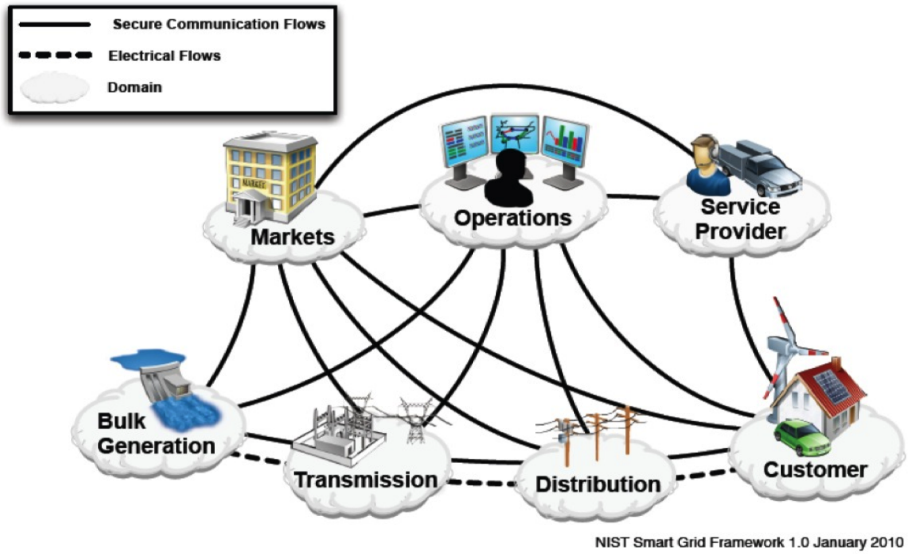

Figure 1.1: NIST Smart Grid Conceptual Model [1]

Customers, Markets, Service Providers, and Operations [1]. The first four domains produce and transfer electricity in two ways, while the other three achieve movement of electricity and provide information to utilities and customers.

Smart grid utilizes different communication technologies to help in improving the grid's fault detection, electricity waste, and self-healing feature. As mentioned previously, the main objectives of the smart grid are to reduce the power losses and stabilize the grid by maintaining the electricity generation-consumption ratio, e.g., the electricity amount in the grid is around a certain level all the time, which increases the efficiency of electricity generation. This upgrade requires merging sensors and measurement devices, such as smart meters and Phasor Measurement Units (PMUs), in the power grid. The main objective of such sensors is to aggregate information about the grid status in widely dispersed areas. On one hand, smart meters, deployed in the customer side, aggregate the electricity consumption for each individual appliance and send the total consumption to the utility. After that, the utility calculates the accurate electricity bill for each consumer. On the other hand, PMUs are high-speed sensors distributed throughout the grid transmission and distribution systems. They monitor the grid status and quickly detect any anomaly behaviors and threats

that could lead to blackouts.

1.2 WAMS

The evolution of the smart grid is driven by increasing power demand, unreliable power flow, distributed system setting, and emerging renewable energy generation. To address these challenges, the smart grid requires dynamic architecture, intelligent algorithms, and efficient mechanisms. Such tasks include generation dispatch decisions on loads or expected demands, estimating the system state and contingency analysis operating every few seconds to few minutes, and protection and control algorithms that operate every few milliseconds. As a consequence, academic and industrial research witnessed a wave of discussion towards the introduction of information and communication technologies with the aim of increasing efficiency of power delivery and management. Therefore, a new measurement system, the so-called Wide Area Measurement Systems (WAMS), has been introduced to power system literature in the late 1980s. This system promises to offer a real-time monitoring system used for synchronized data acquisition in order to control, monitor and manage the performance of the smart grid. Having such a precise understanding of the operation conditions contributes significantly to achieving much-improved performance levels of power systems. The effectiveness of the design of control schemes based on wide-area information can also contribute to better systems utilization.

1.3 WAMS Security

The upgrade of the grid exposes it to cyber-physical security threats such as malicious attacks that can forge the measurements coming from sensors installed in different substations, extract critical information from the readings, or establish Denial-of-Service (DoS)

attacks. In addition, different security threats are introduced to the grid because of its special nature, such as False Date Injection (FDI) attacks that inject fake information about the grid's status to mislead the control center to make wrong decisions that have a negative impact on the grid stability and reliability. In the next subsection, we briefly introduce the main security concerns.

1.3.1 Security Objectives

Cybersecurity tools and techniques are aimed at achieving three primary objectives for the grid's security, *confidentiality*, *integrity*, and *availability* (CIA) described as follows:

- Confidentiality: ensures that only authorized entities have access to critical information. The consumer's privacy and confidentiality are of significant importance in the grid. Eavesdropping on the exchanged messages between sensors and the control center allows attackers to collect information regarding the device type, software version, and configurations. For example, the attacker can gather important information regarding electricity production and consumed power then sell such information to other utilities. As a conclusion, the privacy and confidentiality of exchanged information are important and should be taking into consideration in any proposed security scheme.

- Integrity: ensures that any unauthorized modifications to the transferred data are detected. An attacker can alter or fabricate the transferred information between different domains in the grid. For example, the attacker compromises several measurement units and exploits them to inject false information about the grid conditions. Such an attack, known as False Data Injection (FDI), misleads the control center to make improper decisions for the grid that has negative consequences in different parts of the grid.

- Availability: ensures that critical system information should be available when required. An attacker can target the network resources, e.g., by DoS attacks. In this attack, the attacker aims at blocking, delaying, or corrupting the transmitted information to make it unavailable for legitimate users. For example, the attacker can delay or drop phasor measurements to blind the control center and influence control decisions. Therefore, smart grid networks should be robust to availability attacks as they could lead to severe consequences, such as losing real-time monitoring of the critical power infrastructures, which subsequently lead to large-scale power system disasters, i.e., huge blackouts.

As a result, many research efforts toward building a reliable distributed WAMS architecture have been proposed recently. For example, the data network management task team of North American SynchroPhasor Initiative (NASPI) is working on implementing a distributed WAMS architecture with a focus on protocols, QoS, latency, bandwidth, and security [11]. It is obvious that this distributed architecture will increase the grid reliability by removing single point failures as shown in [12]. Distributed algorithms in power grids have been proposed in recent papers such as [13–17], in the context of distributed optimal power flow, distributed generation, demand side management, and wide area oscillation monitoring. However, this architecture has its drawbacks due to the lack of cyber-physical research. In particular, communication delay, network availability, and its impact on the real-time phasor application need to be studied, which is the purpose of this research. Although a wealth of research has been proposed to address traditional cyber security threats, many solutions do not adequately address the additional constraints required to support the electric grid. Unlike more traditional IT systems, WAMS has many geographically disperse resources with limited physical protection, which leaves them more vulnerable to physical tampering. Moreover, WAMS has strict real-time requirements that make many security mechanisms unacceptable due to its overhead on the communication network. Therefore,

systems with real-time requirements often cannot adopt many security controls.

In summary, merging new communication technologies such as WAMS in future smart grid exposes the grid to many unfamiliar security problems. Such problems are imported from the communication networks in addition to new threats due to the grid nature. In general, the main security risks for WAMS are resources and information availability, data integrity, and data confidentiality. Therefore, in this research, we study the security threats regarding information availability and its impact on the grid's performance. The succeeding sections present our objectives and the thesis contributions.

1.4 Research Objectives

Securing the communication network of WAMS is still an active research. WAMS system might be a target to cyber-attacks or communication network failure that impact the phasor measurements (i.e., delays, packet drop, incomplete measurements, etc.). Therefore, security aspects are extremely important in WAMS as measurements are used for real-time grid supervision, control, and protection. Any altering of measurements may trigger wrong control decisions that might endanger the grid's operations.

Under this setting, the availability, security, and resiliency of the WAMS and the data it carries become crucial to the normal operations of the smart grid. As mentioned previously, the main security goals of a WAMS are to ensure the availability, integrity, and confidentiality of the measurements and the underlying computing and communicating network. Moreover, the data security should be ensured end to end, that is, from the time of data origination at the PMU to the time of use by the control center and/or applications. Security mechanisms solution should not introduce too much additional delay when sending and receiving synchrophasor measurements. Therefore, it becomes essential to understand WAMS communication network and the underlying cyber-physical impacts as well as attack mitigation and recovery techniques. This is exactly what we tried to achieve in this

research.

1.5 Thesis Contribution

This thesis will mainly focus on the relation between WAMS security and IP routing protocol. Mainly, we focus our attention on three fundamental problems. These problems are summarized next and presented in details in dedicated chapters of this thesis.

- First, the increased deployment of synchrophasor technologies increases the effective attack surface available to attackers and exposes WAMS applications. Such applications have strict and stringent delay requirements, e.g., end to end delay as well as delay variation between measurements from different PMUs. We consider delays on the communication networks due to cyber-attacks, which have a negative impact on the transferred measurements causing delays and packet drops, which in turn will impact the applications that rely on the transferred synchrophasors. We present a mathematical model for constructing forwarding trees for PMUs measurements which satisfy the end-to-end delay as well as the delay variation requirements of WAMS applications at data concentrators. We illustrate that simple shortest path routing will result in a larger fraction of data drop and that our method will always guarantee to find a suitable solution. An important goal of this research is to study and characterize the impact of the availability attack on WAMS. To this extent, we use a real-time co-simulation by integrating a communication network simulator (OPNET [18]) with a power grid simulator (Opal-RT/Hypersim [19]). Such co-simulator is integrated, synchronized and equipped with communication capabilities to allow the simulated voltage and current data to flow to PMUs, which allows us to characterize the impact of availability attack.

- Second, we investigate the security of WAMS from a prevention standpoint. As

mentioned earlier, the increased integration of PMUs introduces new vulnerabilities to cyber-attacks, which if exploited by attackers, may have damaging consequences ranging from a local power outage to complete blackout [20, 21]. For instance, [22] showed that a potential network intrusion may cause severe damages, such as cascading failures and massive blackouts similar to the 2003 North-American blackout [5]. Therefore, several algorithms have been proposed to detect the presence of such attacks [23–25]. With detection, actions must be considered to prevent the propagation of cyber-attacks, which is the aim of this thread. Therefore, we propose an optimal IP Multicast tree construction for each connected PMU. Each tree connects the PMU to its set of destinations (PDC, SPDC, data historian, etc.) with the objective of minimizing the likelihood of cyber-attacks propagation while satisfying real-time requirements.

- Finally, we aim at developing a control scheme to compensate for the impact of communication network delays on WAMS applications. The timely collection of phasors from PMUs dispersed across the grid allows to maintain system observability and take corrective actions when needed. This collection is made possible through Phasor Data Concentrators (PDCs) that time-align and aggregate phasor measurements, and forward the resulting stream to be used by monitoring and control applications. Cyber-attacks resulting in the disconnection of PDC(s) from WAMS initiate a loss of its phasor stream and incompleteness in the observability of the power system. We formulate a recovery strategy from loss of PDC(s) in the WAMS network based on the re-routing of disconnected PMUs to functional PDCs. The presented approach is mathematically formulated as a linear program taking into consideration the functionality requirements of the WAMS network, and the use of PMU measurements in the system observability. The approach is tested on standard IEEE test systems.

We compare the collected results with other approaches from the literature. The collected results demonstrate the effectiveness of the presented model in restoring the system observability after a PDC failure due to cyber-attacks.

1.6 Thesis Organization

The thesis is organized as follows. Chapter 2 represents a background on WAMS and its components along with a literature review regarding WAMS security. Chapter 3 addresses the problem of delay attack, a mathematical model for PMU data collection is presented and evaluated with different IEEE test systems. The impact of delay attack and an evaluation using a real-time co-simulator is presented in this chapter as well. Chapter 4 presents the problem of cyber-attack propagation and its relation with IP-multicast routing protocol. A mathematical formulation of multicast trees that minimize the propagation of cyber-attack then evaluated using an IEEE test system is presented in this chapter. In Chapter 5, a recovery scheme for disconnected PDC (after an attack) to restore connectivity with disconnected PMUs and recover their synchrophasor measurements. Finally, A summary of the work reported in this thesis is given in Chapter 6.

2. Background and Literature Survey

2.1 WAMS

Wide Area Measurement Systems were defined by Bonneville Power Administration (BPA) in the late 1980s. In 1995, the US Department of Energy (DOE) and the Electric Power Research Institute (EPRI) started the Wide Area Measurement System (WAMS) Project. WAMS can be defined as ”a system that takes measurements in the power grid at a high granularity, over a wide area and across traditional control boundaries and then uses those measurements to improve grid stability through wide-area situational awareness and advanced analysis” [26]. This can be achieved throughout the collection of measurement values, displayed and processed by human operators and/or control-center applications, from widely distributed sensors. A common type of sensors is the Phasor Measurement Unit (PMU) developed in the early 1980s. PMUs provide a time-stamped voltage and current phasors by utilizing the Global Positioning System (GPS) clock with a sampling rate that ranges from 30 samples per second up to 120 samples per second. These time-stamped measurements are then transmitted to a Phasor Data Concentrator (PDC). The role of a PDC is to aggregate and correlate the time-stamped measurements from different PMUs, then sends the correlated measurements to a Super PDC at the control center as shown in Figure (2.1). PMU measurements play an important role in smart grid operations. The interest in synchrophasor technology has received a great deal of attention in recent years as the need for the best estimate of the power system’s state is recognized to be

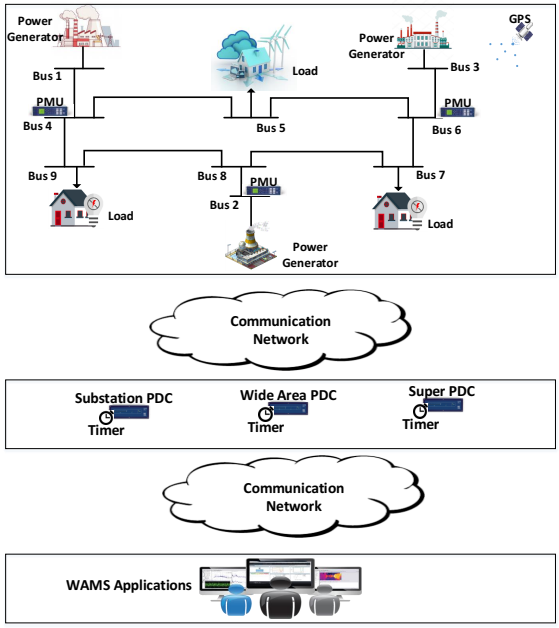

Figure 2.1: Wide Area Measurement System (WAMS)

crucial elements in enhancing the grids performance and resilience to catastrophic failures.

WAMS evolution has made the monitoring of the dynamics of power systems in real-time a promising aspect to enhance and maintain systems stability under stressed operation conditions. Such system is capable of providing a dynamic snapshot of the systems states in real-time and updates it every 20 ms. Having such a precise understanding of the operation conditions contributes significantly to achieving much improved performance levels of power systems.

2.1.1 Benefits of WAMS

The most benefits of WAMS technologies are described as follows:

- Improve the grid's reliability by enhancing situational awareness and advanced applications. For example, WAMS applications can provide early and improved detection of any evolving problems in the grid and allow the system operators to take the required mitigation measures.

- Enhanced integration of distributed energy resources. WAMS can be used to monitor the changes in the grid's behaviour that might be an impact of integrating renewable energy resources.
- Better visualization and assistance tools for operators to manage the system.
- Avoiding large area disturbances.
- Increasing power transmission capability with no reduction of system security.

2.2 SCADA

Supervisory Control And Data Acquisition system is used since the 1970s in the power grid but nowadays more devices that provide more functions are attached to it. The SCADA system can be defined as the technology that enables a user to collect data from distant substations and/or send control commands to those substations. The control center in SCADA systems performs centralized control and monitoring for field devices, which control local operations over long-distance networks. Based on the received information, operator-driven commands are sent to field devices, which control various operations such as collecting data from sensors, monitoring the local environment for alarms, and open and close breakers. The architecture of such system is described in the following subsection.

2.2.1 SCADA Systems Architecture

The following is a list of the major components in SCADA systems [27]:

- Operator: a human operator who monitors the system and controls the operation of the remote plant.
- SCADA Server or Master Terminal Unit (MTU): which is similar to the master unit in a master/slave architecture. The MTU gathers data from a remote site, presents this

data to the operator through a human machine interface, and sends control commands to the remote site.

- Remote Terminal Unit (RTU): functions as a slave in the master/slave architecture. The RTU sends control signals to the device under control such as sensors, acquires data from these devices, and transmits the collected data to the MTU.

- The Programmable Logic Controller (PLC): is a small computer designed to perform logic functions with the ability to control complex processes. Often they are used as field devices due to their flexibility, versatility, and economical use over RTUs.

- Intelligent Electronic Devices (IED): are smart sensors intelligent enough to acquire data, communicate with other devices, and perform local control. IED combines analog input and output, low-level control abilities, memory, and communication system in one device, allowing automatic control at the local level.

- Human Machine Interface (HMI): is the software and hardware that allows the operator to monitor the system's state, modify control settings, and manually override the automatic control in case of emergency.

These components communicate with each other as shown in Figure 2.2. The control center contains the MTU or SCADA server and the communications router in addition to the HMI, workstations, and data historian, all connected by LAN. The control center collects information from field stations, and then displays them to the HMI; actions will be generated based on this information [27]. The field devices perform local control of sensors and actuators, and each field site is equipped with remote access to allow diagnostic and maintenance over a WAN connection. The information is transported between the control center and the field devices using various techniques such as telephone line, satellite, cable, fibber, and radio frequency.

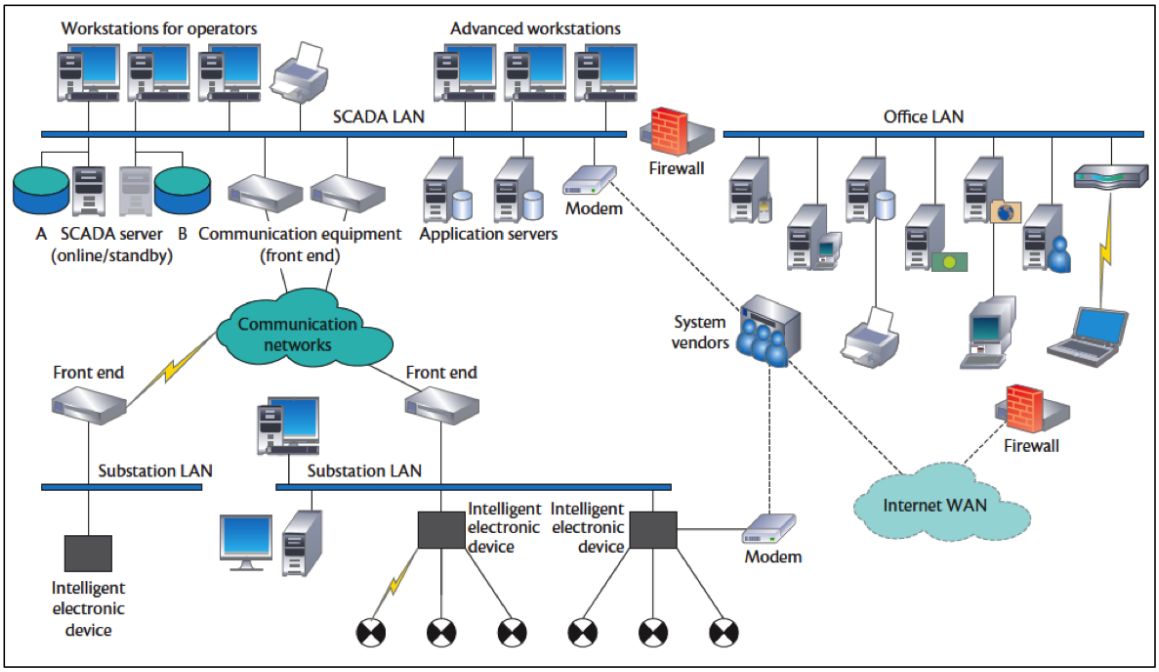

Figure 2.2: Power Grid Control System Architecture [2]

SCADA system collects data from remote terminal units at various substations and relays aggregated measurements to the control center for state estimation. However, various cyber attacks have been reported on SCADA system, resulting in major blackouts, such as the August 2003 Northwest blackout. The 2003 blackout [5] highlighted the need to develop a robust state estimator. Therefore, the integrity of SCADA's state estimation is under threat due to transforming the current power grid to a smarter power grid. This transformation opens the grid to the outside networks through the use of IP-based protocols in the communication system, which could bring complex collaborating attacks. In [28], Liu et al. showed that a new false data injection attack is able to evade bad data detection in today's SCADA system and then introduce an arbitrary error to the state estimation. A recent study in [29] showed that false data injection attacks can cause the state-of-the-art EMS/SCADA state estimator to manipulate more than 50 % of the values without triggering the bad data detection alarm.

2.2.2 WAMS Vs. SCADA

Conventional communication infrastructure, such as SCADA system has limited control and real-time capabilities compared to WAMS. Typically, SCADA provides, at a low transmission rate, uncoordinated and not-fully synchronized system data that does not capture the state of the system at a given moment in time. Rather, the data can provide a good estimate of the system state assuming that the system is in a quasi-steady state. Moreover, such systems may not be able to dynamically monitor the power flow due to the fact that they are based on steady-state power flow. In addition, the time tags of SCADA measurements are not accurate since the clock used in the time tag process is local clocks, which makes it difficult to compare measurements obtained from two different measuring devices. Consequently, SCADA measurements are not suitable for the grid's dynamic monitoring. On the other hand, The measurement rates of PMU are much higher than the rates of SCADA and thus, more suitable for grid dynamics monitoring. Currently, PMUs with reporting rates up to 120 frames/s are mostly available in the commercial markets. Therefore, WAMS emerged as an enhanced measurement technology that complements SCADA by providing a real-time snapshot of the grid dynamics.

2.3 WAMS Components

In general, WAMS has four basic components: PMUs, PDCs, applications that rely on phasor measurements, and a communication network to connect PMUs and PDCs. In the following subsequent sections, each component is described in details.

2.3.1 Phasor Measurement Unit (PMU)

Phasor Measurement Units (PMU) have been increasingly deployed over the past decade as a leading measurement technology for the smart grid transmission system, which opened

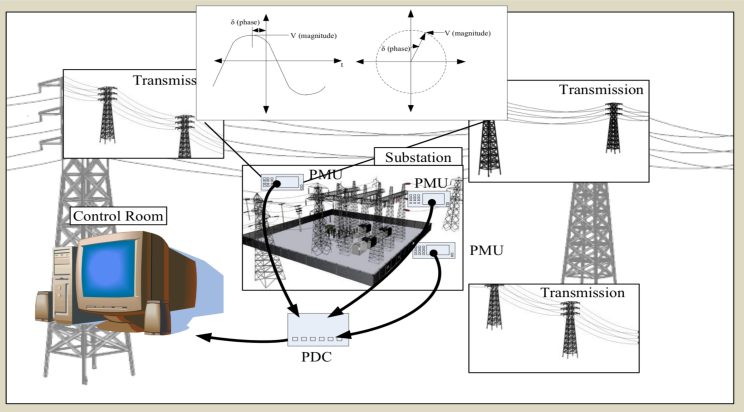

Figure 2.3: Collection of Synchrophasor Data [3]

opportunities to utilize new applications and enhance the grid operations. PMUs measure voltage, current, and frequency at specific locations in the grid as shown in Figures (2.3, 2.4). Voltage and current parameters represent the delivery of electricity from generation to consumers, while frequency is the key indicator of the stability between generation and consumption. PMUs typically sample measurements at a rate of several hundred measurements per second and use this data to calculate the phasor value. A phasor is "a complex number that represents the magnitude and phase angle of the sinusoidal waveforms of voltage or current at a specific point in time" [3]. PMUs include upgraded relay and digital fault recorders (DFRs) that normally capture data during an event such as system fault, equipment failure, or generator tripping.

Synchrophasor is a term used to describe a phasor which has been estimated at an instant known as the time tag of the synchrophasor. In order to obtain simultaneous measurement of phasors across wide area of the power system, it is necessary to synchronize these time tags, so that all phasor measurements belonging to the same time tag are truly simultaneous. Synchrophasors are basically phasors synchronized to an accurate time source. PMUs are synchronized to UTC (Coordinated Universal Time) time, which is a widely used international time standard. The UTC time can be obtained through GPS system, which is a constellation of satellites transmitting signals to the users. The GPS system was

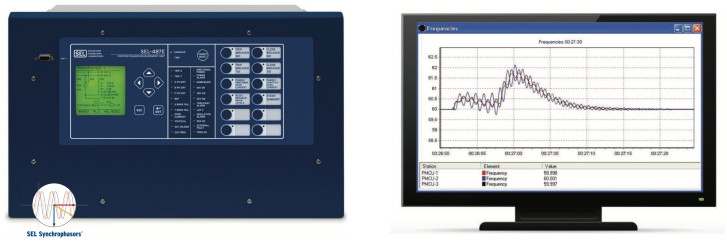

Figure 2.4: Schweitzer Engineering Laboratories (SEL) PMU

Figure 2.5: Schweitzer Engineering Laboratories (SEL) PDC

built by the U.S. Department of Defense (DoD) to make navigation easy with the objective of broadcasting precise time and location information.

2.3.2 Phasor Data Concentrator (PDC)

A PDC as defined in [4] is ”a node in a communication network where synchrophasor data from a number of PMUs or PDCs is processed and fed out as a single stream to the higher level PDCs and/or applications” see Figure 2.5. The PDC groups measurements from different PMUs with the same timestamp into a time-stamped buffer. A new time-stamped buffer is initiated every time the PDC receives phasor measurements with a new

timestamp. When the buffer is full, the PDC forwards the set of measurements to other PDCs and/or Synchrophasor applications. In general, WAMS might suffer from communication delays due to intentional cyber attacks or unintentional communication failures. Hence, the PDC may have to wait for the delayed measurements for its buffer to be full before forwarding the measurements to the applications; this might violate real-time requirements of some applications. A slight modification to this approach has been made where a timer per time-stamped buffer has been added. This timer is the amount of time the buffer is actively waiting for the rest of synchrophasor measurements with the same timestamp. The countdown of the timer starts when the first measurement with a new time stamp arrives at the PDC. Then, the PDC assigns a new buffer to this newly arrived measurement and starts the timer. When the timer goes off, the PDC forwards the received measurements without waiting for the entire measurements to arrive. In case of delays, this wait time ensures that the PDC forwards the phasor measurements in an acceptable time range without waiting for the delayed measurements to arrive. However, this timer introduces the issue of data incompleteness when synchrophasor measurements arriving after the expiration of the PDC timer are dropped at the PDC [30].

A PDC can be found as a stand-alone device or as a function integrated into other systems. According to [4], a PDC can support more than fifteen functions some of them are explained below:

- Data aggregation: this function can be done with or without time alignment. Aggregation with time alignment means that the PDC waits for data from different PMUs or PDCs with the same timestamp then place them in one packet and transfer the packet to a higher level PDC or to an application. On the other hand, aggregation without time alignment refers to periodically transferring synchrophasors with a user-settable transmission interval or data size.

- Data forwarding: this function is performed without data aggregation as PDCs forward data from one input to one or more outputs. Such functionality helps in minimizing PDC latency as some applications require minimum latency.

- Data communications: a PDC is able to communicate with other devices such as PMUs or other PDCs using serial and/or Ethernet networks.

- Data validation: basic data validation may be performed in a PDC by performing time quality, data integrity, and other checks. PDCs may detect and flag any corrupt data before sending it out.

- Data latency calculation: a PDC can calculate and communicates data latency as synchrophasors arrive at the PDC and allow statistical computations for additional latency analysis for assessment of the network performance.

- Output data buffering: in case of communication interruption, a PDC may buffer the output data to minimize the data loss then resends it to the destination after restoring the communication.

- Performance Monitoring: to monitor the quality of transferred data with other devices.

- Duplicate data handling: discarding all duplicate data that arrives at the PDC from different data streams or different communication paths.

- Cyber security: even though cyber security is generally controlled by the application, PDCs should be able to evaluate their security, which goes beyond simply securing synchrophasor communications to securing any communication and access to the PDC.

2.3.3 Communication Network

The communication network plays an important role in the overall performance and functionality of WAMS. It should ensure that synchrophasor measurements are transferred among the required Quality of Service (QoS) of each application. Such network transfer different synchrophasor measurements, which includes phasors, frequency, rate-of-change-of-frequency, analog values, digital values, and status information. The transferred data typically follows a client-server based where a client PDC sends a data request command to a server PMU or other PDC, then the PMU responds with the required data. An IP unicast or multicast data transfer protocol can be used for streaming data between PMUs and PDCs depending on how the network is built.

The multicast function allows an efficient data distribution in the communication network. If a source PMU is sending to multiple destination PDCs, it simply uses a multicast address in the destination field. The synchrophasor packet is then duplicated in the network only as needed to prevent unnecessary bandwidth consumption. However, multicast communication introduced complexity to the network. A multicast routing is needed to establish multicast trees from PMUs to PDCs.

Reliability, security, and efficiency are important criteria of WAMS communication network. Delays in time-critical networks such as WAMS can affect WAMS real-time applications; hence, the grid's performance and stability. Such delay depends on many factors such as network bandwidth, propagation delay, communication medium, etc. Many communication mediums have been considered such as telephone line, satellite, power line communication (PLC), Microwave links, Fibre optic cables. The latest is considered the most attractive medium for WAMS communications as it provides long distance transmissions, low latency, and large bandwidth.

Other than a communication medium, PMUs need to use communication protocol to transfer synchrophasor measurements to destination PDCs. Channel capacity and latency

are an important performance-related feature in a communication medium.

Different protocols have been proposed and continue to evolve. These include some custom protocols (e.g., BPA/PDCstream), IEEE Std 1344-1995 (discouraged), IEEE Std C37.118-2005, IEEE Std C37.118.2-2011, and IEC 61850-90-5 protocols. Currently, the most common used standards are the IEEE Std C37.118.2-2011 and the IEC 61850-90-5.

(1) IEEE Standard C37.118: in 2005, IEEE Standard C37.118-2005 was introduced. It replaces the pervious synchrophasor standard 1344-1995 and provides a synchrophasor definition, compliance testing methods, and message formats to communicate with a PMU. Then, in 2011, two new synchrophasor standards have been introduced and replaced the C37.118-2005. The first standard (C37.118.1-2011) addresses the measurement aspect of PMUs while the second standard (C37.118.2-2011) addresses synchrophasor communications. The latest, defines message types, message formats, and message contents to facilitate real-time synchrophasor communication between PMUs and PDCs. Four types of messages have been defined as follows:

- Data frame: contains measurements estimated by PMUs.
- Configuration frame: contains machine readable information
- Header frame: contains human readable information.
- Command frame: contains machine readable information such as appropriate actions to be taken.

(2) IEC 61850-90-5: provides protocol for exchanging synchrophasor information between PMUs and wide area monitoring and control applications.

(3) IEEE C37.244-2013: describes the functional requirements of PDCs.

A high speed and intelligent communication infrastructure is the key to make time-critical WAMS applications feasible in practice.

2.3.4 WAMS Applications

Synchrophasor measurements are used to support many applications, ranging from visualization of information and alarms for situational awareness, to applications that provide sophisticated analytical, control, or protection functionalities. Applications, such as dynamics monitoring, use full-resolution, real-time data along with the grid models to support both operating and planning functions. The application(s) locally display measured frequencies, primary voltages, currents, real and reactive power flows, and other quantities for system operators. Synchrophasor applications have been widely discussed as a possible way to promote smart grid operations to a more efficient and responsive level [30]. Therefore, to realize the full potential of synchrophasor technologies, advanced applications that improve the grid monitoring, control, and protection are needed [3]. Such applications require more PMUs to be installed at different parts of the grid. For instance, under the U.S Department of Energy's smart grid initiative, several thousand PMUs are being scheduled to be installed in the coming few years [13].

This increased deployment of PMUs will increase the volume of transferred data per second. Moreover, the effectiveness of these synchrophasor measurements is subject to communication timing guarantees. As a result, utility companies and independent system operators are trying to understand how to efficiently process and utilize the gigantic volumes of real-time phasors. Hence, the current centralized WAMS architecture will no longer be sustainable under such data explosion, and a completely distributed architecture needs to be developed as a natural choice [31].

Under distributed WAMS, synchropasor applications are implemented in a distributed fashion on multiple PDCs. Such applications, put stringent time requirements in terms of data delays in comparison to the conventional SCADA systems; Table 2.1 shows different synchrophasor applications. In addition, these applications require phasor measurements from distributed PMUs to be sent to the corresponding PDCs in a synchronous fashion in

Table 2.1: Synchrophaor Applications

Application	Online/Offline	Class	Local/Wide	Purpose	Sampling rate	Latency
Wide-Area Monitoring and Visualization	Online	Class C	Wide area	Monitoring	30 samples/second	NA
Oscillation Detection	Online	NA	Local/Wide area	Control	30 samples/second	200 ms
Frequency Stability Monitoring	Online	Class C	NA	Monitoring	30 samples/second	2-4 se
Voltage Stability Monitoring	Online	Class C	Wide area	Monitoring	30 samples/second	1 sec
State Estimation	Online	Class B	NA	Monitoring/Control	30 samples/second	Less than 100 ms
Islanding and Restoration	Online	NA	Wide area	Control	30 samples/second	50 msec
Post-Event Analysis	Offline	Class D	NA	Monitoring	NA	NA

real-time [32]. Each PDC receives phasor measurements from a set of PMUs distributed in different parts of the grid with varying distances, which can impact the required time for sending their phasor measurements. Moreover, the shared IP network that sends the phasor measurements to PDCs provides services to other sensors such as Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs), a video for surveillance purpose, and Voice over IP applications [33]. Moreover, based on [34], network delays in WAMS communication have a negative impact on the grid performance especially on closed-loop power system performance.

In summary, as PMUs are being increasingly deployed, it is crucial for WAMS to transfer the phasor measurements from different PMUs to their destinations (PDC, SPDC, synchrophasor applications) in a secure, efficient, and timely manner. A PDC receives synchrophasor measurements from one or more PMU through a data communication network (e.g. wireless or wired IP-based network) as presented in the NASPInet architecture [35]. Generally, WAMS requires a high-speed and intelligent communication network to collect synchronized measurements from distributed PMUs. Thus, power line and microwave communication were proposed earlier as WAMS communication technologies; however, these technologies have their limitations regarding reliability, scalability, and robustness [36]. Therefore, optical fiber communication that allows low latency, high bandwidth, and low loss attracted WAMS applications to transmit data from PMUs to PDCs [21]. Currently, PMUs transmit their measurements to a pre-defined set of PDCs in

a hierarchical manner using IP Unicast network transmission [37]. However, with the increasing deployment of PMUs and PDCs along with the rising number of applications that rely on PMU measurements, the existing configuration suffers from several drawbacks such as message delays, limited latency and throughput, and limited scalability [38]. Therefore, a new configuration, e.g. IP Multicast, is needed to meet the new requirements [39–42]. This configuration addresses the fact that PMUs are classical multicast sources since each PMU sends a continuous data stream to a number of destinations (i.e., PDCs, Super PDCs, data historian, etc.). Thus, it is more reasonable to consider IP Multicast protocols for carrying PMU measurements; IP multicast minimizes packet replication and thus is more bandwidth efficient.

2.4 Literature Survey

2.4.1 False Data Injection Attack

Attacks targeting the smart grid critical processes, such as state estimation, have attracted lately an increasing attention in the research community. Until recently, it was assumed that the system state estimation is immune to cyber attacks. However, a recent work by Liu et al. [28] demonstrates that in the presence of an intelligent attacker equipped with the knowledge about the grid topology, false data can be injected into sensor measurements to introduce an arbitrary change in the estimated states without being detected. This new class of attacks is called False Data Injection (FDI) attack. Due to the ability of the attacker to change the system state without being detected, an increasing effort has been directed toward the detection of such an attack. In [23], protecting a set of carefully selected sensor measurements by, for example, guards or video monitoring, is proposed as a countermeasure against FDI attacks. However, selecting the set of measurements to be protected is an NP-hard problem [43]; thus, recent studies have proposed various methods to select the

set of sensor measurements for protection. The authors of [24] developed a greedy algorithm to obtain the optimal set of sensor measurements that need to be protected to evade cyber-attacks. In [43], a graphical method has been developed to optimally select the set of sensor measurements to be protected in order to defend against cyber-attacks. The authors in [25] present a generalized likelihood ratio test to implement a detection algorithm for cyber-attacks targeting the state estimation. In [20], a detection and identification approach has been proposed to detect cyber-attacks in PMUs using the Expectation-Maximization algorithm. After detection, appropriate measures need to be taken to avoid the propagation of cyber-attacks.

Next, we present a literature review of different proposed approaches that aim at constructing an FDI attack under different circumstances such as the knowledge of the attacker or his limited resources. As we have mentioned previously, the work by Yao et al. that addressed the FDI attack assumed that the attacker had full access to the Jacobian matrix H, which represents the network topology of the power grid. Moreover, it assumed that the attacker had the ability to physically tamper with a specific number of sensors and manipulates their measurements. However, [44] presented a formal model for state estimation verification while considering different attack attributes such as specific target, limited capability, etc. In contrast, [24] proposed a unified formulation to construct the optimal attack vector a, using a minimum number of manipulated measurements, by developing a low complexity attack strategy that outperforms the naive ℓ_1 relaxation. However, this approach required a relaxation of the constraints on the basic problem statement. Thus, [45] proposed a graph-theoretic algorithm that presented the optimal solution to the optimal attack vector without any relaxation.

Moreover, the current research direction has been shifted to consider different scenarios, where the attacker either has partial or zero knowledge of the network topology. In [46], the authors proved that an FDI attack can be constructed even when the attacker has no

knowledge of the system topological information. In this case, the attack can be launched only if the measurement placement has a special structure such as bridging edges. On the other hand, when this special structure is not available, the attacker needs to have partial knowledge about the network topology to be able to launch an undetectable FDI attack. In [47], they studied the ability of the attacker to construct an attack vector with limited knowledge about the network topology. Moreover, [48] proposed an approach that can exploit the subspace structure of the system measurements in the case where the attacker has limited knowledge about the network topology.

The majority of research is considering the DC power flow model due to its simplicity and ability to derive the exact solution in most cases. Another reason behind the wide use of the DC model is that AC state estimation is more complicated, due to several differences. First, AC power flow solutions are usually obtained through iteration, whereas in DC model they are generally obtained in closed-form. Second, DC power flow state estimation is based on active power flow, while the AC model is based on both active and reactive power flow. Third, the DC model's state variables consider voltage phase angles, but the AC model considers both voltage phase angles and voltage phase magnitude as states.

However, the AC power flow model is widely used in the power grid; thus, recent researches have considered AC state estimation [49] [50]. The ability to construct an FDI attack against power system state estimation when it uses the more practical AC model has been examined in [50], where the attacker is required to collect some online data during the attack implantation. Based on these online data, the attack is divided into two classes: perfect and imperfect attacks. In a perfect attack, the attacker can accurately obtain the online data needed for state estimation. In an imperfect attack, the attacker may obtain online data with errors. An analytical mechanism for vulnerability assessment of AC state estimation was proposed in [49], where the use of the system physical propreties can help the grid operator to mitigate FDI attacks. From the attacker's perspective, an algorithm

based on a graph that determines the set of measurements which need to be compromised in order to minimize the effort of the attacker has been proposed [49].

Using AC power flow state estimation provides advantages to the system operator if the attacker does not have the knowledge of the system configuration; otherwise, the attacker will be able to launch an FDI without being detected.

The problem of finding the smallest number of measurements the attacker needs to compromise has been proved to be an NP-hard problem [24]. In [51], Yang et al. transformed the NP-hard problem to the Minimum Subadditive Join problem, which is NP-hard as well.

In the following subsections, we describe the problem of finding the optimal set of measurements to be protected, followed by a literature review on the current proposed approaches.

(1) *Secure Measurements*

The conventional method to defend against FDI attack is by securing a set of measurements to evade malicious injections, either by use of guards, video monitoring, or a tamper-proof communication system. This may acquire additional fees for installation and maintenance in large power grids. Many approaches have been proposed to tackle the problem of finding the optimal protection set of measurements while minimizing the cost at the same time. In [23], the authors explored the ability of the operator to verify the values of the selected state variables, which provides indirect protection for the sensor measurements that most affect the value of the state variables.

The authors of [52] addressed this issue and proposed a sequential method to find a minimum set of protected measurements for the protection of any set of state variables. However, the enumeration-based method is of very high complexity in large-scale power systems. Therefore, it is essential to develop a method that can protect a

set of state variables that have a greater social/economic impact once compromised. The authors of [53] proposed the use of PMUs as well to provide direct voltage measurements at specific buses to mitigate FDI. In [54], the authors showed that no undetectable attack can be launched if the power grid is observable from the protected set of measurements.

(2) *Secure Transmission Lines*

Another approach which has recently emerged to defend against FDI attack is to limit the attacker's knowledge of the network topological information by changing some software/hardware parameters, such as transformer taps in transmission lines. This protection method has a lower operation cost in comparison to protecting a set of measurements. However, not all transmission lines can be covert, such as lines missing transforms taps and breakers.

It was shown in [55] that intentional topology disturbance may enable the grid operator to detect an FDI attack using a traditional Bad Data Detection (BDD) residual test. However, a random topology disturbance may not dissolve the possibility of an undetectable FDI attack. The work of [56], which is an early version of [46], limits the attacker's knowledge of the network topology by protecting the information of a minimum number of transmission lines. Where the solution of the optimal protection problem can be obtained by solving a Steiner tree problem where many well-investigated algorithms can be used [56]. As we have mentioned earlier, not all transmission lines can be kept covert. Therefore, a mixed defense strategy, that considers both the proposed covert topology and the protection of a set of measurements, is proposed when the information about the transmission line cannot be covert. In this case, the mixed defending strategy can be done by solving the optimal measurements protection after converting available covert transmission lines into a flow

measurements [57].

The work of [46] proposed the use of Covert Topological Information (CTI) to limit the attacker's knowledge about the network topology such that no undetectable FDI attack could be launched. Furthermore, a mixed defending strategy similar to [56] has been proposed where in [46], the authors extended the method in [56, 57] by considering a general case with varying cost to protect each actual measurement. A positive weight to each edge in the graph is added based on the difficulty of protecting the measurement it is mapped to. Hence, the problem becomes similar to solving a Steiner tree with a minimum edge weight sum. Finally, the optimal mixed defense strategy can be obtained by solving the equivalent secure meter selection problem [57].

In [47], the attacker can launch an undetectable FDI attack when he has limited but structured topological information. Therefore, the grid operator needs to make a wise decision on which part of the topological information needs to be covert, while the rest can be revealed to the public.

Moreover, multiple false data attack detection algorithms have been proposed, mainly with a focus on maximizing the detection probability and attack damage control. In a study at coordinated data injection [54], a Generalized Likelihood Ratio Test (GLRT) was proposed to detect and localize an attack in which the attacker utilizes a graph-theoretic approach. Signal processing and machine learning are also used in the detection of FDI attacks [58]. Another approach [59] formulated the detection problem as a low-rank matrix recovery and completion problem and then solved it using convex optimization. In this approach, the authors' main contribution is considering time series measurements in the detection problem, which is different from other approaches that focus on single time measurements. Formulating the problem of detecting FDI as a metric separation problem has been proposed in [60]. Using distributed state estimation to detect an FDI attack has

been proposed in [61, 62], in which the power system is divided into many subsystems using clustering algorithms. Then a Chi-squares test is used in each subsystem to detect an FDI attack, and if detected the result works as a guide for the graph update. Finally, a decentralized detection approach is designed based on a Markov graph of bus phase angles [63]. This approach is based on the insight that under normal operation the Markov graph matches the power grid graph; otherwise, the system is under attack and an alert should be triggered.

Other research deploys current IDS [64, 65], such as behavior-based [66] and bloom-filter-based [64], which monitor the abnormal behavior using predefined rules to detect the attack.

2.4.2 Multicast Tree Construction

The problem of constructing multicast trees has received considerable attention in the past. Such tree construction has been considered in different networks such as ad-hoc networks, mesh networks, and wireless sensor networks. In [67], a multicast tree construction for wireless ad-hoc network is proposed; however, such networks are different than the smart grid in the sense that such network requires a flexible and efficient routing due to the dramatic changes in the network topology and limited bandwidth. In [68], the multicast tree construction is formulated as one of computing a directed Steiner tree of minimal cost. Such solution can be beneficial to applications in which a tree is used repeatedly for several large-volume transactions and where the user is desirous of bounding the cost whatever the nature of the network, such as on-demand video services, news distribution, and stock distributions. In [69], a multicast tree that meets the quality of service requirements of real-time interactive applications operating in a high-speed packet switch environment has been proposed.

Moreover, the problem of routing multicast traffic with real-time constraints has been studied in [70], and heuristics to compute low-cost trees which guarantee an upper bound on the end-to-end delay have been developed. For a survey and extensive simulation study of a large number of existing multicast algorithms and an evaluation of their performance in high-speed environments, the reader is referred to [71]. Moreover, QoS-based and security-based routing scheme for smart grid communications has been investigated to meet smart grid applications requirements. In [72], a detailed multicast routing implementation is proposed for smart grid voltage control. Routing is formulated as an optimization problem assuming a simplified model of the physical system and heuristic solution approaches are applied. In [73], the authors propose a hybrid structure routing architecture to enable the resilience, robustness, and efficiency of the smart grid. This routing protocol is based on distributed optimization of the QoS along individual routing paths. In [74], the authors construct QoS multicast tree to deliver control messages from the controller to a set of remote devices while minimizing the end-to-end delay. In [30], an analysis of the communication network for WAMS applications with a focus on end-to-end delay is presented. The aim of such analysis is to quantify the end-to-end delay given a specific communication network (envisioned design for the Swedish transmission grid). In [75], the authors proposed a flocking-based multicast routing for the smart grid with efficient situational-awareness for network traffic. The aim is to balance the end-to-end delay and bandwidth for WAMS communication. However, considering the time variation between the arrival of synchrophasor measurements; hence, the PDC timer in the tree construction has not been addressed.

2.4.3 Attacks Targeting PMUs

Recently, increasing efforts have been devoted to understanding cyber attacks targeting PMUs. In [76], the authors study a GPS spoofing attack, targeting the measurement system, where the attacker sends a forged GPS signal in order to cause variation in the measured

PMU phasors. Such an attack has no available defense mechanism, which threatens critical applications that rely on PMU measurements as presented in [77]. Moreover, PMU data spoofing, denial of service and WAMS communication links damage are studied in [21], where a co-simulation platform is developed to assess the impact of such attacks on the power grid.

2.4.4 The Impact of Delay and Data Incompleteness

The impact of data incompleteness has been addressed recently in [78], where the impact of network delay on the incompleteness of the data was studied and a trade-off between delay and data incompleteness with different PDC timer setup was presented. In [79], the impact of the network delay and data incompleteness in WAMS has been studied. The authors in [34], developed a control scheme to compensate the network effects in WAMS such as induced network delays, packet disordering, and data packet drops. In [80], the impact of data incompleteness on the system state estimation due to cyber-attack has been addressed. Moreover, several studies have considered the problem of stability of power systems with time delays [81, 82]. Congestion (intentional or not) along the communication links may result in constant/random packet delays. As a result, queue lengths become very large, buffers overflow, packets get delayed or dropped, resulting in incomplete information at the application side [83]. These issues lower the data quality and can even impact the performance of WAMS applications

2.4.5 Cyber-attack Propagation

Propagation of attacks on shared communication network is studied in [37, 84]. Cyber-attacks in open grid environment are addressed in [85], and a Mixed Integer Linear Programming (MILP) optimization model to avoid the attack propagation is proposed. In the context of PMUs network, Mousavian *et al.* propose in [37] a probabilistic mitigation

model to find an optimal response to cyber attacks. A so-called threat level, the probability of a PMU to be contaminated through a compromised PMU, is calculated. Then a MILP response model is formulated to minimize the threat level of all connected PMUs at a certain time by disabling PMUs that are likely to be compromised. However, such model does not consider the interaction between the routing in IP multicast and the attack propagation; such interaction is addressed in this report.

2.4.6 Attacks Targeting PDC

Cyber-attacks targeting PMUs and their impact on the grid's operations has received much interest from the research community recently [86–88]. However, little work has focused on attacking PDCs and its impact on WAMS applications. In general, when a PDC is identified as compromised and disconnected from the communication network, more severe consequences can occur in comparison with attacking a PMU. On one hand, when a PMU is detected to be under attack, to prevent the propagation of the attack the compromised PMU will be disconnected from the network, which means losing its measurements. On the other hand, attacking and disconnecting a PDC means losing all measurements sent to that PDC even though the reporting PMUs might not be compromised and can still send trusted synchrophasor measurements. Therefore, to minimize the impact of cyber-attacks (disconnecting a compromised PDC), measurements from trusted PMUs need to be re-routed to other connected PDCs immediately, instead of waiting for the compromised PDC to be fixed.

To restore the services of PMUs that were lost because of disconnecting a compromised PDC, [89] proposed a two stage self-healing mechanism to connect trusted PMUs with un-compromised PDCs in order to restore the observability of the power system while minimizing the latency to configure the network. Several constraints have been considered in this approach during the re-connection process such as hardware resources capacities

in both communication and transmission network e.g., the size of the forwarding table and the connection space of PDCs. However, an important feature of the PDC has not been considered, the so called PDC timer. A timer is a time at which a PDC is actively waiting for measurements with a certain time stamp to arrive. When the timer goes off, the PDC drops delayed measurements that arrive after the expiration of the timer. Such a feature should be considered in the rerouting process of measurements from un-compromised PMUs to other connected PDCs to avoid rerouting measurements to a PDC that has an expired timer. Moreover, rerouting a measurement to a PDC that arrive earlier than original measurements sending to that PDC can invoke the timer to start earlier which might affect other original measurements sending to that PDC.

3. Enhancing WAMS Communication Network Against Delay Attacks

3.1 Introduction

Phasor Measurement Units (PMUs) have been increasingly deployed over the past decade as a leading measurement technology for the smart grid transmission system. Such deployment has opened opportunities to utilize new applications and enhance the grid operations. As mentioned in Chapter 2, PMUs provide time-stamped high-resolution measurements of voltage and current phasor, frequency, and phase angle from different parts of the grid. These time-stamped measurements are then transmitted to a Phasor Data Concentrator (PDC). The role of the PDC is to aggregate and correlate the time-stamped measurements from different PMUs, then sends the correlated measurements to a Super PDC at the control center. This synchrophasor system is used to monitor, control, and protect the power grid by collecting measurement values, displayed and processed by human operators and/or applications, from widely dispersed areas.

Synchrophasor applications have been widely discussed as a possible way to promote smart grid operations to a more efficient and responsive level [30]. Therefore, to realize the full potential of synchrophasor technologies, advanced applications that improve the grid monitoring, control, and protection are needed [3]. Such applications require more PMUs

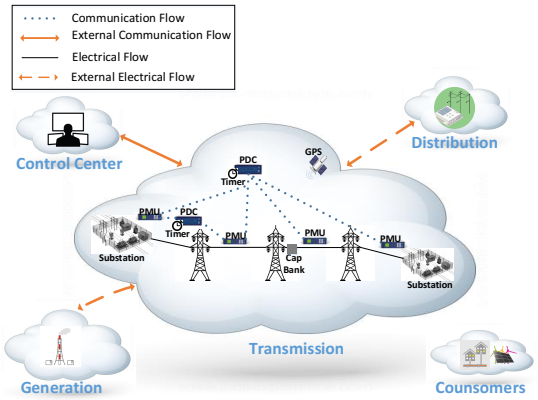

Figure 3.1: Wide Area Measurement System

to be installed at different parts of the grid. For instance, under the U.S department of Energy's smart grid initiative, several thousands PMUs are being scheduled to be installed in the coming few years [13]. This increased deployment of PMUs will increase the volume of transferred data per second. Moreover, the effectiveness of this synchrophasor measurements is subject to communication timing guarantees. As a result, utility companies and independent system operators are trying to understand how to efficiently process and utilize the gigantic volumes of real-time phasors. Hence, the current centralized WAMS architecture will no longer be sustainable under such data explosion, and a completely distributed architecture need to be developed as a natural choice [31].

The increased integration of PMUs introduces new vulnerabilities to cyber-attacks, which if exploited by attackers, may have damaging consequences ranging from local power outage to complete blackout. Recently, multiple PMU vulnerabilities have been reported by Arbiter [90]; these vulnerabilities can cause a Denial of Service (DoS) as identified in the Arbiter Systems Power Sentinel PMU. Moreover, some PMU vendors such as the National Instruments PMU (NI Grid Automation System) [91] provides Linux-based PMUs that can be subject to linux?worm/malware attacks (such as Moose and Darlloz.A). Many research efforts toward building a secure and reliable distributed WAMS architecture have been proposed recently [11,92]. For example, the data network management task team

of North American SynchroPhasor Initiative (NASPI) developed a reference communication infrastructure called NASPI network to support synchrophasor delivery and specify recommended smart grid data delivery requirements including latency and reliability [11]. However, if these technologies are not accompanied with appropriate security enforcement, they may also create new vulnerabilities in the network, leaving it open to a wide range of cyber-physical attacks [93]. Therefore, approaches and methods to improve the network performance against attacks are necessarily needed, which is the purpose of this chapter.

As mentioned in Chapter 2, the PDC timer is the amount of time the buffer is actively waiting for the rest of synchrophasor measurements with the same time stamp. The countdown of the timer starts when the first measurement with a new time stamp arrives at the PDC. Then, the PDC assigns a new buffer to this newly arrived measurement and starts the timer. When the timer goes off, the PDC forwards the received measurements without waiting for the entire measurements to arrive.

In case of delays, this wait time ensures that the PDC forwards the phasor measurements in an acceptable time range without waiting for the delayed measurements to arrive. However, this timer introduces the issue of data incompleteness when synchrophasor measurements arriving after the expiration of the PDC timer are dropped at the PDC [30]. In general, the value of the timer depends on the application that uses those measurements. For example, control applications have really strict delay requirements; thus, the value of the timer should be small. However, with monitoring application or post disturbance analysis applications the value of the timer could vary. Such stringent delay requirements is needed to achieve one of WAMS main objectives, which is proving real-time monitoring and control based on synchronized measurements arriving at high sampling rate.

Currently, the shared data network that forwards the phasor measurements to PDCs provides services to other sensors such as Remote Terminal Units (RTUs) and Intelligent

Electronic Devices (IEDs), a video for surveillance purpose, and Voice over IP applications [33]. Therefore, this shared network can contribute to larger network latency for a particular PDC. Figure (3.2) shows a WAMS with multiple PMUs communicating with different PDCs. In particular, for PDC (n), two PMUs are sending their measurements through a communication network. Each PMU might experience different network latency; thus, the packet arrival times of both PMUs at the PDC might vary. Synchrophasor measurements arriving after the expiration of the PDC timer will be dropped leading to a negative impact on the real-time WAMS applications.

(1) *Contribution:* this chapter is devoted towards investigating WAMS communication delays and their impact on WAMS real-time applications. It has been shown that non-functional properties, such as data delay and packet drops, have a negative impact on the system functionality [94]. Therefore, with the aforementioned communication challenges in mind, we propose a way to enhance WAMS performance. We consider a system with multiple PMUs, each communicating with one or more PDCs, using a shared data network. Our approach is to develop a robust routing method for gathering measurements from PMUs at PDCs while satisfying the end to end delay as well as delay variation at the PDC between measurements coming from different PMUs. In other words, our approach is to minimize the number of invalid or dropped measurements at the PDC, i.e., measurements arriving after the timeout period expired at the corresponding PDC. We believe therefore there is a strong interplay between the routing paths (delays along the paths) for gathering the measurements and the value of timeout period. An oblivious routing method to delay constraints may not deliver timely measurements at the PDCs and result in data incompleteness affecting several WAMS applications and ultimately the system observability. Therefore, our focus is to construct delay-aware measurement gathering paths between PMUs and PDCs to address the data incompleteness problem. Moreover, we validate the proposed model

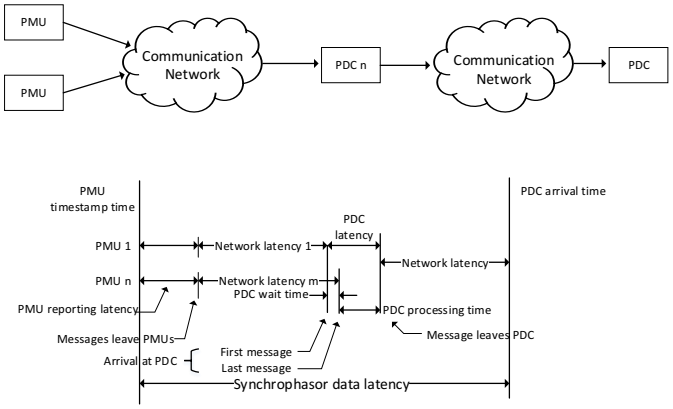

Figure 3.2: Synchrophasor System [4]

using a real-time co-simulation platform.

3.2 Problem Description

In this section, we start with a simple example to illustrate the delay and data incompleteness problem. Figure (3.2) shows a WAMS that consists of PMUs communicating with a PDC through a data network. As mentioned previously, WAMS requires a reliable and fast communication network to meet the real-time requirements. Therefore, delays on the transferred measurements due to a communication failure or cyber-attacks are critical especially for real-time synchrophasor applications (e.g., state estimation and power system oscillation damping controller). Further, depending on how measurements are routed in the network, they might experience different delays and hence may arrive after the expiration of the PDC timer.

As mentioned before, the IP multicast routing addresses the fact that PMUs are classical multicast sources since each PMU sends a continuous data stream to a number of destinations (i.e., PDCs, Super PDCs, data historian, etc.). Thus, it is more reasonable to consider IP Multicast protocols for carrying PMU measurements; IP multicast minimizes packet replication and thus is more bandwidth efficient. Therefore, the relation between the

communication delay and the IP routing protocol, which is important for the collections of synchrophasor measurements, need to be addressed. Moreover, as mentioned earlier, data incompleteness due to such delays should be minimized, which is the aim of this chapter.

Based on that, we present a tree construction model for gathering PMUs packets with the objective of minimizing the number of invalid measurements during a PDC timer. It is to be noted that a shortest tree construction, as will be shown later, may not achieve this objective. Our tree construction is delay-aware and will ensure that the number of invalid measurements at PDCs is minimized by properly selecting efficient paths for gathering the measurements from PMUs.

3.2.1 Problem Definition

Consider a distributed WAMS with a set of PMUs $N_u = \{u_1, ..., u_{|N_u|}\}$, a set of PDCs $N_c = \{c_1, ..., c_{|N_c|}\}$. In addition, we consider a data network that connects PMUs to PDCs. The system can be abstracted to a directed graph $G = (N, E)$, where E is a set of edges and N is a set of nodes $N = N_u \cup N_c \cup N_r$. The notion N_r represents a set of routers connecting PMUs and PDCs where $N_r = \{r_1, \ldots, r_{|N_r|}\}$. Each PDC c_i is receiving synchrophasor measurements from a set of PMUs. Let S_{c_i} be the set of PMUs sending their measurements to PDC c_i. Similarly, each PMU u_i is sending its measurements to a set of destinations PDCs D_{u_i}.

As we mentioned earlier, each WAMS application has a different delay and data requirements. In the case of network delays, some phasor measurements might arrive at the PDC after the expiration of the PDC timer and those measurements will be dropped leading to data incompleteness. A straightforward solution is to increase the value of the timer at the PDC to receive all the required measurements; however, such a solution might violate the real-time requirements of some applications that may not tolerate any delay such as power oscillation damping monitoring.

For example, power oscillation application has two different modes, the first one is associated with a single generator or plant against the rest of the power grid are referred to as local modes. The second one is the inter-area oscillation that appears when a group of generators in one area are oscillating against a group of generators in another area and often suffers from poor damping. As WAMS technology allows synchrophasor measurements from remote locations to be available at the control center in a high sampling rate, it opens the opportunity of using remote signals to design more efficient control applications such as inter-area power system oscillation damping control. However, such applications have strict delay requirements and time delay can degrade the system performance and diminish the effectiveness of the control system; which may result in complete system instability [95, 96]. Therefore, in the case of delays, increasing the value of the PDC timer to minimize the number of dropped packets at the PDC due to the expiration of this timer might violate those delay requirements (up to 30 milliseconds for the round trip that is from the time of measurements up to the time of reaction). Increasing the timer value will increase the time delay as the time delay between the instant of measurements and the time of the measurement being available at the damping controller would deteriorate the control performance of such applications.

Therefore, the aim of this chapter is to construct trees and collect phasor measurements from PMUs while respecting the end-to-end delay (from PMUs to PDC) as well as the delay variation between measurements coming from different PMUs. Such solution, if found, will maximize the number of valid synchrophasor measurements per PDC timer, which will be significant to applications relying on these measurements. Further, in presence of cyber attacks deliberately increasing the delay on some links along some paths in the forwarding trees, our method can reconstruct the forwarding trees to avoid such links and therefore enhance the system performance against such attacks.

3.3 The Mathematical Model

In this section, we present the proposed tree construction model to connect PMUs and PDCs. Let C_{ij} be the capacity of the communication link (i, j), f_{ij}^{u} be the flow from PMU u on edge (i, j), δ_{uc} be the end-to-end delay from PMU u to PDC c (which depends on the total flow on each link), and δ_{Th} be the end-to-end delay threshold (which depends on the WAMS applications). Let x_{ij}^{u} be a binary variable such that:

$$x_{ij}^{u} = \begin{cases} 1 & \text{if edge } (i,j) \text{ is in } u\text{'s tree} \\ 0 & \text{otherwise} \end{cases}$$

Let y_{ij}^{uc} be a binary variable such that:

$$y_{ij}^{uc} = \begin{cases} 1 & \text{if the path to } c \text{ from } u \text{ traverses edge } (i,j) \\ 0 & \text{otherwise} \end{cases}$$

As mentioned previously, our objective function is to maximize the number of received "valid" measurements within a PDC timer. Let $\beta_{u_i c}$ be a binary variable equal to

$$\beta_{u_i c} = \begin{cases} 0 & \text{if measurement } u_i \text{ is valid} \\ 1 & \text{otherwise} \end{cases}$$

A measurement u_i is valid if its end-to-end delay (from the source PMU to the destination PDC) is less than a specified threshold (δ_{Th}), and if it arrives at the PDC within an acceptable time window (defined by the timer which is initiated when a PMU measurement with new time stamp arrives first, see Figure (3.3)); this can be translated mathematically

as follows:

$$\delta_{u_i c} \leq \delta_{Th} \tag{3.1}$$

$$\delta_{u_i c} \leq \delta_{u^* c} + t_{out} \tag{3.2}$$

where t_{out} is the PDC timer, and $\delta_{u^* c}$ is the delay of the *first* received measurements with a new time stamp. In other words, $\delta_{u^* c} = min(\delta_{uc})$. Knowing the time of the first received measurements and the timer length for a PDC is useful for calculating the number of received measurements within a timeout period as described in equation (3.2). To write this (min expression) into a Linear Program format, we introduce the following variables. Let $x_{u_i c}$, $x^c_{uu'}$, and $x'_{u_i c}$ be binary variables such that:

$$x_{u_i c} = \begin{cases} 0 & \text{if } \delta_{u_i c} \leq \delta_{Th} \\ 1 & \text{otherwise} \end{cases}$$

$$x^c_{u_i u'} = \begin{cases} 0 & \text{if } \delta_{u_i c} \leq \delta_{u' c} + t_{out} \\ 1 & \text{otherwise} \end{cases}$$

$$x'_{u_i c} = \begin{cases} 0 & \text{if } \sum\limits_{u' \neq u} x^c_{u_i u'} = 0 \\ 1 & \text{if } \sum\limits_{u' \neq u} x^c_{u_i u'} > 0 \end{cases}$$

Therefore, the mathematical model (which minimizes the number of invalid received measurements) can be formulated as follows:

$$\text{Minimize} \quad \sum_{u_i} \beta_{u_i c} \quad \forall c \in N_c$$

Subject to

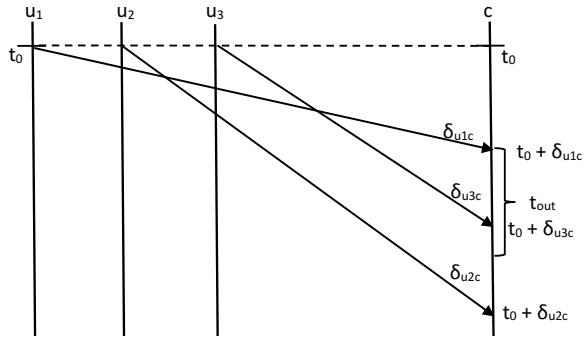

Figure 3.3: Starting Point of The PDC Timer

- *The number of valid measurements within a timer period:* to determine the number of received"valid" synchrophasor measurements, with the same time stamp, within a PDC timeout period.

$$\delta_{u_ic} \leq \delta_{Th} + x_{u_ic} \times M, \quad \forall u_i \in N_u, c \in N_c \tag{3.3}$$

$$\delta_{u_ic} \geq \delta_{Th} + (1 - x_{u_ic}) \times M, \quad \forall u_i \in N_u, c \in N_c \tag{3.4}$$

Constraints (3.3)and (3.4) are the linearization of the decision variable x_{u_ic}, where measurement (u_i) is valid if its delay to PDC (c) is less than δ_{Th} and M is a big real number.

$$\delta_{u_ic} \leq \delta_{uu'} + t_{out} + x^c_{u_iu'} \times M, \quad \forall u_i \in N_u, c \in N_c, u' \in N_u, u_i \neq u' \tag{3.5}$$

$$\delta_{u_ic} \geq \delta_{uu'} + t_{out} - (1 - x^c_{u_iu'})M, \quad \forall u_i \in N_u, c \in N_c, u' \in N_u, u_i \neq u' \tag{3.6}$$

Constraints (3.5) and (3.6) are the linearization of the decision variable $x^c_{u_iu'}$, where $\delta_{u'c}$ is the delay from all PMUs (u') to PDC (c). Measurement (u_i) is valid if it arrives at PDC (c) within the t_{out} value, which starts at the arrival of the first received

measurement with a new time stamp (see Figure (3.3)).

$$\sum_{u' \neq u} x^{c}_{u_i u'} > x'_{u_i c} - 1, \quad \forall u_i \in N_u, c \in N_c \tag{3.7}$$

$$\sum_{u' \neq u} x^{c}_{u_i u'} \leq x'_{u_i c} \times M, \quad \forall u_i \in N_u, c \in N_c \tag{3.8}$$

$$\sum_{u' \neq u} x^{c}_{u_i u'} \geq 0, \quad \forall u_i \in N_u, c \in N_c \tag{3.9}$$

Constraints (3.7), (3.8), and (3.9) specify that when the measurement (u_i) arrives within c's timer, then the value of $x'_{u_i c}$ should be equal to zero. Finally, the value of $\beta_{u_i c}$ can be described as follows:

$$\beta_{u_i c} = x_{u_i c} + x'_{u_i c}, \quad \forall u_i \in N_u, c \in N_c \tag{3.10}$$

- *Delay Constraints*: this ensures that the constructed forwarding trees satisfy the applications' delay requirements. As defined in the IEEE Std. C37.118.2, the total delay of synchrophasor data is composed of a communication delay (t_d) and terminal processing delays (t_{PMU}) and (t_{APP}) as shown in Figure (3.29). Moreover, some literature further divides the total delay into six terms as in (3.11), [97].

$$\begin{aligned} t_{delay} &= t_{PMU} + t_d + t_{APP} \\ &= t_{PMU} + (t_{PDC} + t_{RN} + t_{BN}) + t_{APP} \end{aligned} \tag{3.11}$$

where t_{PMU}, t_{PDC}, and t_{APP} are considered as PMU latency, PDC latency and the time the application takes to process and respond to the received synchrophasors, respectively (see Figure (3.4)). On the other hand, t_{RN} and t_{BN} are communication

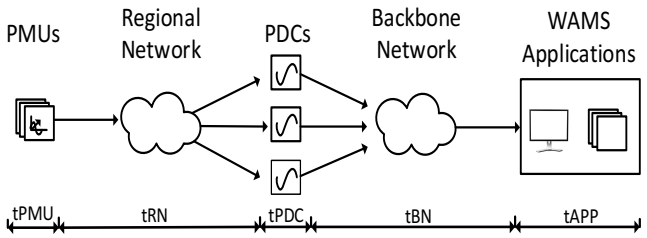

Figure 3.4: WAMS Delays

delays over regional and backbone networks. In this chapter, we focus on the regional networks, while the backbone network is considered as a black box [97].

In particular, the processing delays can be limited to small ranges or even fixed to constant as proposed in the PDC standard [4]. However, the communication delay is normally uncertain and stochastic [98]. Therefore, many research activities study the stochastic nature of communication delays through experiments or simulations and then, model the average or stochastic values [99–101]. For example, Zhang *et al* measure the communication delay of Guizhou Power Grid in 100 seconds and model the communication delays as constant [99]. The latency of a process bus network of a substation is tested in a laboratory environment in [101], and the impact of data loss and latency on digital protection are analyzed. In [97], the authors demonstrated the dependency of synchrophasor application reliability on the system architecture while considering data delay and losses.

The end-to-end communication delay from a source to a destination can be described as the sum of processing delay, queuing delay, transmission delay, and propagation delay on each link along the path connecting the source (PMU) and destination (PDC). Processing delay can be neglected since routers are considered as forwarding nodes (no processing), measurements processing occurs at end nodes (PDCs) [102].

Moreover, the propagation delay is assumed to be no more than 1 microsecond [102]. Thus, each link ij along the path experiences a delay Δ_{ij} computed as follows:

$$\Delta_{ij} = t^{ij}_{trans} + t^{ij}_{que} + t^{ij}_{prop} \tag{3.12}$$

where t^{ij}_{trans} and t^{ij}_{que} are the transmission delays and queuing delays on link ij respectively. The transmission delay t^{ij}_{trans} on (i, j) is calculated as follows:

$$t^{ij}_{trans} = f_{ij}/C_{ij}, \quad \forall (i, j) \in E \tag{3.13}$$

where f_{ij} is the total flow (e.g., number of packets carrying measurements) on link (i, j). The queuing delay (of packets at node i which are forwarded on link ij) can be determined by the traffic behaviour and can be approximated as follows:

$$t^{ij}_{que} = 1/(\mu - \rho_{ij}), \quad \forall (i, j) \in E \tag{3.14}$$

where μ is the mean service rate (e.g., average number of packets processed per second by the router) which depends on the port speed and ρ_{ij} is the average rate of traffic arriving to this port; ρ_{ij} is modelled as a function of the flow conservation variables y^{uc}_{ij}. Finally, the propagation delay t^{ij}_{prop} is calculated by the distance between nodes and the speed of light in the communication medium. Now, the end-to-end delay can be calculated as follows:

$$\delta_{uc} = \sum_{(i,j)\in E} y^{uc}_{ij} * \Delta^{ij}_{trans}, \quad \forall c \in N_c, u \in N_u \tag{3.15}$$

The PDC processing delay can be calculated as follows:

$$t_{PDC} = t_{out} + t_{alig} + t_{buff} \tag{3.16}$$

where t_{out} is the timer of the PDC, t_{alig} is the time for processing and alignment at PDC c, and t_{buff} is communication system buffering and error correction.

- *Flow Conservation Constraints:* to construct the forwarding trees between PMUs and PDCs we use the following constraints:

$$\sum_{j:(i,j)\in E} y_{ij}^{uc} - \sum_{j:(j,i)\in E} y_{ji}^{uc} = \begin{cases} 1 & \text{if } i = u \\ -1 & \text{if } i = c \\ 0 & \text{if } i = r \end{cases}$$

$$y_{ij}^{uc} \leq x_{ij}^{u} \quad \forall (i,j) \in E, u \in N_u, c \in N_c \tag{3.17}$$

$$x_{ij}^{u} \leq \sum_{c} y_{ij}^{uc} \quad \forall (i,j) \in E, u \in N_u, c \in N_c \tag{3.18}$$

$$f_{ij}^{u} \leq \sum_{c} y_{ij}^{uc} \quad \forall u \in N_u, (i,j) \in E \tag{3.19}$$

$$f_{ij}^{u} \geq y_{ij}^{uc} \quad \forall u \in N_u, c \in N_c, (i,j) \in E \tag{3.20}$$

The first constraint represents the flow conservation constraints for y_{ij}^{uc}, constraints (3.17) and (3.18) describe the relation between y_{ij}^{uc} and x_{ij}^{u} as they ensure that if there is a path between PMU u and PDC c on link (i,j), then link (i,j) is a link in the constructed forwarding tree. Constraints (3.19) and (3.20) describe the relation

between y_{ij}^{uc} and f_{ij}^{u} as if link (i,j) is on the path from u to c, then this link should have flow from PMU u.

$$f_{ij}^{u} \geq x_{ij}^{u} \quad \forall u \in N_u, (i,j) \in E \tag{3.21}$$

$$x_{ij}^{u} - (f_{ij}^{u}/M) \geq 0 \quad \forall u \in N_u, (i,j) \in E \tag{3.22}$$

Constraint (3.21) and (3.22) describe the relation between x_{ij}^{u} and f_{ij}^{u}, if there is no flow on link (i,j) then link (i,j) is not on the tree of PMU u.

- *Subtour Elimination Constraint*: to avoid loops we use the following subtour elimination constraint:

$$\sum_{i \in S} \sum_{j \in S} x_{ij}^{c} \leq |S| - 1, \quad \forall S \subset N, 2 \leq |S| \leq |N| \tag{3.23}$$

where S is a subset of nodes such that $S \subseteq N$.

- *Edge Capacity Constraint*: to ensure that the constructed tree satisfies edge capacity constraints we use the following constraint:

$$\sum_{u} f_{ij}^{u} \leq C_{ij}, \quad \forall (i,j) \in E \tag{3.24}$$

- *Number of flows to PDC c:* to ensure that the number of flow on the last link that connects the PMUs to PDC c is equal to the number of PMUs sending to that PDC

$$\sum_{u} f_{ic}^{u} = S_{c_i} \quad \forall c \in N_c, (i,c) \in E \tag{3.25}$$

where S_{c_i} is the number of PMUs sending to PDC c_i

- *Number of flows from PMU u:* to ensure that each PMU is sending to its set of destinations

$$\sum_{i}\sum_{c} y_{ic}^{uc} = D_{u_i} \quad \forall c \in N_c \tag{3.26}$$

where D_{u_i} is the number of destinations (PDCs) for PMU u_i

Throughout our numerical evaluation, we solve the following optimization model:

$$\text{Minimize} \quad \sum_{u_i} \beta_{u_i c}$$

Subject to

Constraints (3) - (11), (16), and (18) - (28)

3.4 Numerical Results

We evaluate our tree construction method presented earlier and compare it with a base method that uses shortest trees for carrying the measurements from PMUs to their destination PDCs. The shortest tree is computed using Dijkstra's method [103]. Moreover, we compared our proposed tree model with the multicast trees proposed in [75]. We consider the following IEEE test systems: the IEEE 14-bus, IEEE 24-bus, and IEEE 30-bus, New England 39-bus, and 57-bus test systems. Our numerical results are divided into two parts: performance evaluation and cyber-attack impact analysis. For the performance evaluation,

we compare the number of invalid measurements by varying the value of the timeout period at PDCs. The timeout period at the PDC determines how long the PDC will have to wait after it receives the first measurement (a measurement with new time stamp) from a PMU before it sends the collected measurements in its buffer to a super PDC or to the control center. A tight value for this period implies a small allowable delay variation between different measurements, thus ensuring their timeliness. However, at a tight value, the tree construction becomes a hard task and the forwarding tree may contain more links, increasing the communication cost. Moreover, we compare the number of invalid measurements using different set of destinations for each PMU. Then, we compare the average number of links per forwarding tree as well as the computation cost for finding solutions using different set of destinations. Finally, we varied the timeout value for the PDCs to mimic WAMS applications different delay requirements.

On the other hand, for the cyber-attack impact analysis, we simulate an attack on a communication link and study the impact on the constructed trees. Then, we validate our model using a real-time co-simulation. Our numerical evaluations are conducted using CPLEX solver version 12.4 on a Windows 7 machine running at 2.67 GHz with 6.00 GB RAM.

The electric power grid is considered completely observable when all of its system states are uniquely identified [104]. The system states can be estimated at the control centre based on the received measurements from sensors across geographically dispersed areas. With the increased deployment of PMUs, a lot of research work has been proposed to find the minimum number of PMUs along with their optimal locations to ensure system observability [105]. Different scenarios have been studied when finding the optimal PMU placement such as normal conditions, single PMU outages, single branch outages, and with or without conventional measurements. In this chapter, we consider the optimal PMU placement under normal operating conditions with no conventional measurements as

Table 3.1: Optimal PMU number and placement for each test system

Test System	Number of PMUs	Bus Locations
IEEE 14-bus	4	2,6,7,9
IEEE 24-bus	7	2,3,8,10,16,21,23
IEEE 30-bus	10	2,3,6,9,10,12,15,19,25,27

presented in [105]. Table 3.1 shows the optimal number of PMUs needed for observability for each test system and corresponding bus locations. Each PMU sends its measurements to a randomly generated set of destinations.

3.4.1 Performance Evaluation

We start by comparing the number and percentage of received invalid measurements for each test system as shown in Table (3.2). As we mentioned previously, a measurement is valid if it arrives within the PDC timeout period and its end-to-end delay is less than the end-to-end delay threshold (For example, a typical PDC timer for the state estimation is 50 ms [80]). We compare the number of measurements during different PDC timer values (30 ms, 40 ms, 50 ms, and 60 ms) for each test system. Clearly, a larger value for the PDC timeout will result in a smaller number of invalid measurements, as it is easier to find forwarding trees with loose delay variation; however, some WAMS applications, such as control applications, can not tolerate large values for the PDC timer. Although when the value of (t_{out}) is large, the shortest path tree and the multicast trees in [75] can generate trees with no or small number of invalid measurements, however, when (t_{out}) is small then the other methods generate trees with large number of invalid measurements even though we can, through our model, find different routes in the network to minimize the number of invalid measurements (see Table (3.2)). For example, the number of invalid measurements at PDCs (using the shortest path) is equal to 4 when $t_{out} = 30ms$ (for IEEE 14-bus test system), which is 40% of the total number (10) of measurements (see

Table 3.2: Number and Percentage of "invalid" Measurements

Test System	Trees	30 ms		40 ms		50 ms		60 ms	
IEEE 14-bus	Proposed Model	0	0 %	0	0 %	0	0 %	0	0 %
	Shortest Path	4	40 %	3	30 %	1	10 %	1	10 %
	Wei and Kundur [75]	0	0 %	0	0 %	0	0 %	0	0 %
IEEE 24-bus	Proposed Model	1	5 %	0	0 %	0	0%	0	0%
	Shortest Path	5	23 %	3	14 %	2	9 %	0	0 %
	Wei and Kundur [75]	2	9%	6	14 %	3	9 %	1	4%
IEEE 30-bus	Proposed Model	0	0%	0	0%	0	0 %	0	0 %
	Shortest Path	5	13 %	4	10 %	1	3 %	1	3 %
	Wei and Kundur [75]	13	36%	5	13%	1	3%	0	0%

Table 3.2). Our model however will delay the arrival of the first measurement (that will initiate the timer) by forwarding it through a longer path to compensate the variation in the delay between measurements and allow those measurements to make it within the time out period of the PDC. In fact, intentionally forwarding the PMU data through a longer path endangers those time-sensitive WAMS applications; however, in our model we have an end-to-end delay constraint to ensure that even when using longer route the end-to-end delay does not exceed a specific threshold to ensure the strict delay requirements of WAMS applications. On the other hand, forwarding measurements along shortest trees will violate the constraint of delay variation and hence more measurements arriving after t_{out} period are deemed invalid.

Then, we varied the value of T_{out} for different PDCs in the same run to mimic the delay variation of WAMS application as shown in Table (3.3).

Next, we study the effect of the tree construction on the communication cost, which is measured by the number of communication links added on the forwarding trees. Indeed, more links along the forwarding trees imply higher network bandwidth consumption. In Table (3.4), we compare the average number of links per tree for the shortest path tree, the multicast tree in [75], and the proposed tree model. The table shows only a slight

Table 3.3: The number of Invalid measurements and the average number of links per tree using different t_{out} values

Test System	Invalid Measurements	Links per Tree
IEEE 14-bus	0	9
IEEE 24-bus	0	12
IEEE 30-bus	0	14

Table 3.4: Average Number of Links per Tree

Test System	Trees	30 ms	40 ms	50 ms	60 ms
IEEE 14-bus	Proposed Model	9	8	8	9
	Shortest Path	8	8	8	8
	Wei and Kundur [75]	9	9	9	9
IEEE 24-bus	Proposed Model	14	12	12	12
	Shortest Path	12	12	12	12
	Wei and Kundur [75]	14	14	14	14
IEEE 30-bus	Proposed Model	16	16	16	16
	Shortest Path	15	15	15	15
	Wei and Kundur [75]	15	15	15	15

increase in the average number of links on the forwarding trees constructed by our model. Moreover, we randomize the selection of destinations for each PMU and investigate the impact on the number of links per tree as shown in Table (3.5). It is clear that changing the set of destinations doesn't change the average number of links per tree as the proposed model manages to construct trees with different destinations while keeping the number of links and hence the cost of the tree minimized.

Table 3.5: Average Number of Links per Tree (different set of destinations)

Test System	Trees	30 ms	40 ms	50 ms	60 ms
IEEE 14-bus	Proposed Model	9	8	8	8
	Shortest Path	8	8	9	8
IEEE 24-bus	Proposed Model	13	13	12	12
	Shortest Path	12	13	12	12
IEEE 30-bus	Proposed Model	16	15	16	16
	Shortest Path	15	15	116	15

Table 3.6: End-end delay (in Milliseconds)

Test System	Trees	30 ms	40 ms	50 ms	60 ms
IEEE 14-bus	Proposed Model	90	95	98	96
	Shortest Path	88	88	88	88
	Wei and Kundur [75]	82	82	82	82
IEEE 24-bus	Proposed Model	62	85	63	64
	Shortest Path	63	63	63	63
	Wei and Kundur [75]	60	60	60	60
IEEE 30-bus	Proposed Model	72	71	69	72
	Shortest Path	72	72	72	72
	Wei and Kundur [75]	65	65	65	65

Table 3.7: CPU run-time using the proposed tree model (Mathematical Model Vs. Heuristic Approach)

Test System	Trees	60 ms	50 ms	40 ms	30 ms
IEEE 14-bus	Proposed Model	0.03 sec.	0.03 sec.	0.17 sec.	0.52 sec.
	Heuristic	0.121 sec.	0.131 sec.	0.119 sec.	0.122 sec.
IEEE 24-bus	Proposed Model	17.60 sec.	41.17 sec.	113.65 sec.	837.38 sec.
	Heuristic	0.140 sec.	0.145 sec.	0.138 sec.	0.143 sec.
IEEE 30-bus	Proposed Model	3.20 sec.	89.93 sec.	2202.44 sec.	$>$150 hours
	Heuristic	0.204 sec.	0.208 sec.	0.222 sec.	0.204 sec.
IEEE 39-bus	Proposed Model	NA	NA	NA	NA
	Heuristic	0.237 sec.	0.236 sec.	0.241 sec.	0.245 sec.
IEEE 57-bus	Proposed Model	NA	NA	NA	NA
	Heuristic	0.297 sec.	0.314 sec.	0.306 sec.	0.331 sec.

Then, we compared the average end-to-end delay of the proposed model with the end-to-end delay of the other approaches as shown in Table (3.29). It is clear that even though our proposed model has larger delay in some cases, however, the proposed model manages to maintain the end-to-end delay less than the threshold for all cases.

Next, we compare the computational time of our proposed tree model for each test system as shown in Table 4.15. We experiment with different values of (t_{out}) and we observe that increasing the value of the timer decreases the run time to compute the model.

Table 3.8: CPU run-time using the proposed tree model

Timer	IEEE 14-bus	IEEE 24-bus	IEEE 30-bus
60 ms	0.03 sec.	17.60 sec.	3.20 sec.
50 ms	0.03 sec.	41.17 sec.	89.93 sec.
40 ms	0.17 sec.	113.65 sec.	2202.44 sec.
30 ms	0.52 sec.	837.38 sec.	$>$ 540000 sec.

Table 3.9: Average CPU run-time using the proposed tree model (different set of destinations)

Timer	IEEE 14-bus	IEEE 24-bus	IEEE 30-bus
60 ms	0.172 sec.	1.14 sec.	168.81 sec.
50 ms	0.256 sec.	20.916 sec.	93.242 sec.
40 ms	0.576 sec.	2133.67 sec.	4834.355 sec.
30 ms	0.514 sec.	4419.548 sec.	$>$77685.88 sec.

However, when the value of (t_{out}) decreases and becomes very small, the run time of the model increases substantially. The reason of the increase is that at smaller values of (t_{out}) it becomes quite difficult for the model to find a tree that can guarantee delay variation for the measurements, and possibly this tree may not exist. For example, when $t_{out} = 30ms$, the model ran for more than 150 hours for the IEEE 30-bus system and did not generate a solution.

Clearly, the proposed model is hard to scale for larger test systems. To this extent, we propose a heuristic approach to tackle this problem. In this approach, the tree construction will be done off line where for each PMU we generate a number of random multicast trees. For example, for each PMU we have a set of possible trees (first shortest path, second shortest path, etc.) to connect this PMU (u_i) with its set of destinations PDCs. Then, we use the following mathematical model to choose the best tree combination for each PDC such that the number of invalid measurements is minimized.

3.4.2 Mathematical Model for Tree Selection

First, for each PMU we generate a set of possible multicat trees (first shortest path, second shortest path, etc.) offline. Then we take the generated trees as an input to the following mathematical model. The result of such model is a set of trees that satisfies the end-to-end delay constraint and has the minimum number of invalid measurements for each PDC.

Mathematical Model:

Let τ_u be a set of possible trees for PMU$_u$, $\tau_u = \{T_{i1}, T_{i2}, ..., T_{iM}\}$. For each PMU u sending synchrophasor measurement to PDC c there is a set of M possible paths $\{P_{uc}^m\}_{m=1..M}$ from PMU u to PDC c. Let t_{um} be binary variable such that: the n^{th} tree in τ_u (the set of all trees for PMU u).

$$t_{um} = \begin{cases} 0 & \text{if the } m^{th} \text{ tree of PMU } u \text{ is selected} \\ 1 & \text{otherwise} \end{cases}$$

And γ_{um}^{ij} is a parameter defined as follows:

$$\gamma_{um}^{ij} = \begin{cases} 0 & \text{if the } m^{th} \text{ tree of PMU } u \text{ traverses link}(i,j) \\ 1 & \text{otherwise} \end{cases}$$

Then $\gamma_{um}^{ij} * t_{um}$ will be equal 1 only if the m^{th} tree of PMU u is selected and traverses link (i, j). Therefore, the mathematical model (that selects PMUs' tree with minimum number of invalid measurements) can be formulated as follows:

$$\text{Minimize} \quad \sum_{u_i} \beta_{u_i c}$$

Subject to

Table 3.10: Number and Percentage of "invalid" Measurements

Test System	Trees	60 ms		50 ms		40 ms		30 ms	
IEEE 39-bus	Shortest Path	3	7 %	3	7 %	6	14 %	7	16 %
	Heuristic	0	0 %	1	2 %	2	4 %	5	11 %
IEEE 57-bus	Shortest Path	3	4 %	6	9 %	7	11 %	8	12 %
	Heuristic	1	1 %	1	1 %	3	4 %	4	6 %

$$\sum_{m} t_{um} = 1, \quad \forall u \in N_u \tag{3.27}$$

$$f_{ij} = \sum_{u,m} \gamma_{um}^{ij} * t_{um}, \quad \forall (i,j) \in E \tag{3.28}$$

$$\Delta_{ij} = f_{ij}/C_{ij}, \quad \forall (i,j) \in E \tag{3.29}$$

$$\delta_{uc} = \sum_{m} \sum_{(i,j) \in P_{uc}^{m}} (t_{um} * \Delta_{ij}), \quad \forall u \in N_u, c \in N_c \tag{3.30}$$

Constraints (3) - (10)

Constraint (3.28) calculates the total flow over link (i, j), which means the number of selected trees of all PMUs going though link (i, j). Constraint (3.29) computes the delay on link (i, j), and Constraint (3.30) calculates the end-to-end delay form PMU u to PDC c.

Then, we assess how well our proposed heuristic perform compared to the shortest tree construction as shown in Table (3.10). Moreover, we compare the CPU run time of the proposed model Vs. the heuristic approach in Table (3.7).

3.4.3 Delay attack Impact Analysis

In this subsection, we analyze the impact of delays attacks (due to cyber-attacks) on the constructed trees. Even though WAMS communication network tends to be a dedicated Intranet, this does not mean that such networks are immune to cyber-attacks. For instance,

removable media such as USB drives can be used to carry malware and hack computers to be used as sources of other attacks such as denial of service (DoS). Moreover, increasing the number of mobile devices can be used as a malicious medium and we cannot rule out the possibility that utility employees directly inject attacks into the network [8, 106]. A delay attack may be caused by flooding the network with a huge amount of redundant data traffic to consume the target (communication link) resources such as network bandwidth; this means that a very limited bandwidth is left for the useful data. In this case, the measurements data will experience longer communication delays and as a result may be dropped by the PDC. As a consequence, this can blind the system operators and increase the vulnerability of the grid to further attacks or inappropriate operations. More importantly, regardless to any consequences, the impacts of acting on incorrect or missing information will have already propagated into the rest of the system. At this stage, it may already be too late to avoid a wide-area power outage within the grid [107].

First, we consider the IEEE 14-bus test system where 3 PDCs and 4 PMUs are installed to ensure the system observability as shown in Figure (3.5). The communication links are placed in parallel with the transmission lines and each bus is represented as a communication node which can send, receive and route measurements [80]. For a detailed model of realistic communication for the IEEE 14-bus standard test system readers are refereed to [108]. Moreover, in [109], designing a communication network for the smart grid and communication requirements of different applications has been investigated. In [110], an IP based decentralized communication infrastructure that addresses different applications requirements is proposed. Finally, the requierements for a communication infrastructure in the smart grid has been addresed in [31, 102, 111–114, 114].

Each PMU is sending its measurements to a set of destination PDCs, and the values of (δ_{Th}) and (t_{out}) are $120\ ms$ and $60\ ms$, respectively. Then, we simulate an attack on a communication link (chosen based on the frequency of its appearance in the constructed

trees) in the network; due to this attack, additional delays will be added to that link. First, we simulate an attack on link $(6, 12)$ by inducing 20 ms to that link and construct our trees. However, we observe that such delay did not have a big impact on the constructed trees; thus we increased the induced delay to 40 ms and observe the constructed trees. We consider PMU 4 (installed at bus 9) as shown in Figure (3.5) that sends measurements to all installed PDCs. The constructed trees before and after the attack are shown in Figure 3.7. We notice that attacking a communication link will change the constructed trees and a new path has been constructed. Figure (3.6) shows the number of invalid measurements as we vary the amount of injected delays. Clearly, the larger the delay value, the more invalid measurements and hence more dropped packets at PDCs. In the case of IEEE 30-bus system, the model was always able to avoid the attacked link and construct forwarding trees that will meet the delay constraints. Moreover, we simulate an attack on a communication link in the network; such attack causes link disconnection. Figure (3.8) shows the number of invalid measurements due to link disconnection. It is clear that disconnecting a communication link will result in some measurements being dropped at the PDC. As disconnecting a communication link might force some measurements to follow other routes (with larger delay) to avoid the disconnected link resulting in dropped measurements at the PDC due to the expiration of the PDC timer or violating the end-to-end delay. It should be noted that if one PMU frame is discarded by the PDC due to a time-out, then the computations of WAMS applications have to be performed based on the most recently available PMU data frames, and these measurements are one or more reporting cycle old. We notice that even when attacking more than one communication link, the proposed model manages to maximize the network performance against attack by minimizing the number of invalid measurements even for larger network (IEEE 30-bus) where the number on invalid measurements remains zero after injecting 100 ms.

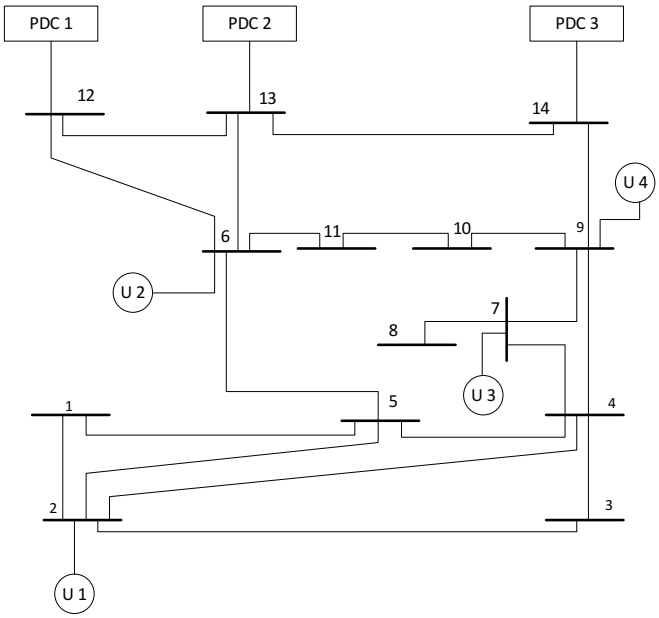

Figure 3.5: Placement of PMUs for the IEEE 14-bus System

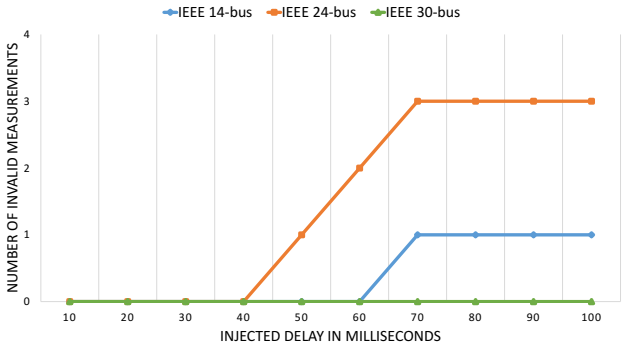

Figure 3.6: Number of "Invalid" Measurements After Attack

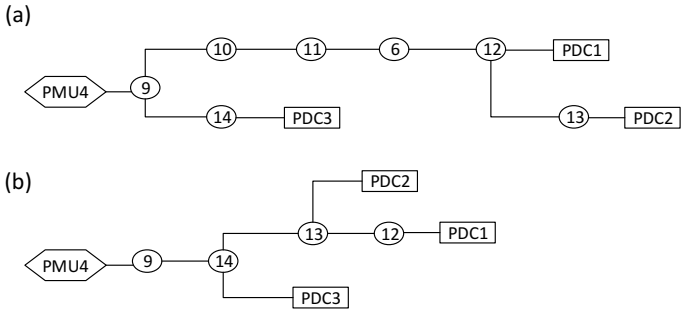

Figure 3.7: Tree of PMU 4. (a) before delay attack, (b) after delay attack

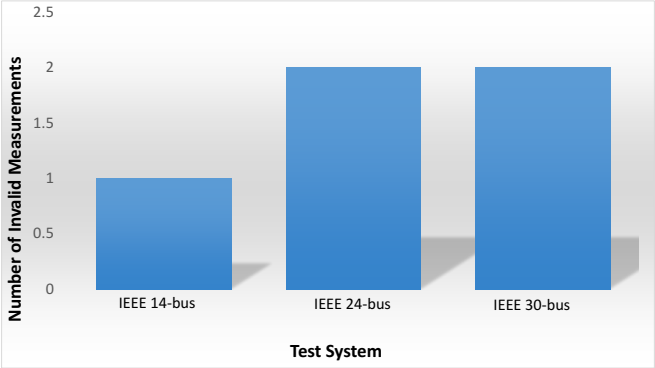

Figure 3.8: Number of ”Invalid” Measurements After Line Disconnection

3.4.4 Validation on Real-time Co-simulator

In this subsection, we validate the performance of the proposed model in comparison with shortest path tree using a real-time co-simulation testbed. In this testbed, a hardware-in-the-loop approach to simulate the power grid real-time dynamics is used. Our hardware-in-the-loop (HIL) testbed is enabled with four PMUs from different manufacturers. Those PMUs receive the analog output from Hypersim, and sample the measurements in the form of C37.118 traffic. The traffic generated by the PMUs is routed to two physical PDCs, one considered as local and the other as regional. The local PDC aggregates the measurements, and forwards them to the regional PDC. The regional PDC sends the received measurement to the control center.

For the power simulator, we use OPAL-RT [115] Hypersim machine that is capable of simulating models of the power grid using the AC power model in real time. By assigning sensors to different components of the power model we are able to collect measurements that reflect the power system status. Such measurements are collected and sampled in the form of C37.118 [116] standard. On the other hand, to simulate the communication network component of the smart grid, we used OpenStack [117] technology, which provides a various set of services that meets the needs of the smart grid. Then, using OpenStack we built a virtual network that interfaces with the PMUs, PDCs, and the control center. The

control center constitutes of different applications that monitor and control the state of the grid. Our control center constitutes of a software from SEL [118], Synchrowave Central.

Experimental Setup: Our experimentation setup consists of the IEEE 14-bus test system, and a coupled communication network. Through this setup, we aim at studying the impact of delay attack on WAMS. To enable this study, we installed two PMUs. PMU_A measures the magnitude, phase angle, frequency, and rate of change of frequency (ROCOF) for the three phases, while PMU_B is placed to collect similar measurements to those collected by PMU_A. Using IEEE C37.118 [116], the two PMUs send the collected measurements to PDC1. Then, PDC1 aggregates the received C37.118 data using the associated time stamps, and sends them to the control center. The communication network used for this setup is depicted in Figure (3.13). To simulate delay attack on WAMS through PMU measurements, we introduced an attacker in the form of a transparent bridge capable of injecting delays in the communication link between the first hop router of PMU_B and the last hop router of the PDC. Therefore, following the shortest path tree (minimum number of hops) without considering end-to-end delay and the delay variation at the PDC will result in packets drop (PMU_B) as seen in Figures ((3.9), (3.11)). On the other hand, under attacks, our model manages to find alternative route such that the end-to-end delay and delay variation constraints are satisfied as shown in Figures ((3.10), (3.12)).

Such packets drop can impact the performance of WAMS applications(e.g., state estimation, power system oscillation damping, etc.). For example, considering a transmission line fault detection application where synchrophasor measurements (synchronized voltages and currents at two terminals of a transmission line) are used to estimate fault location. If a measurement from one PMU is dropped due to delay attack then the performance of such application will be affected as old measurements from previous sampling cycles will be used to estimate the fault, which does not reflect the actual system in real-time.

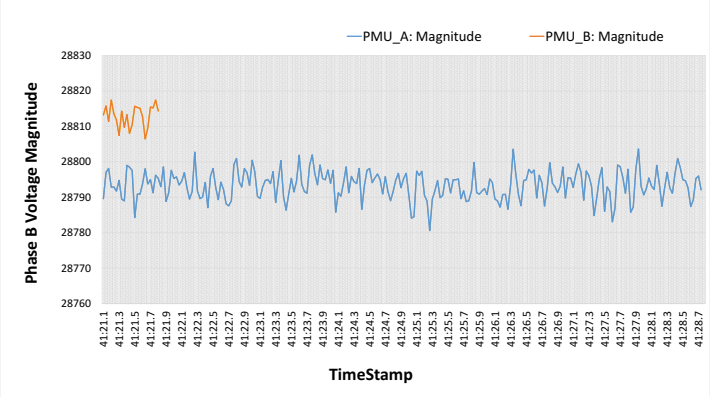

Figure 3.9: Voltage Magnitude Using Shortest Path Tree

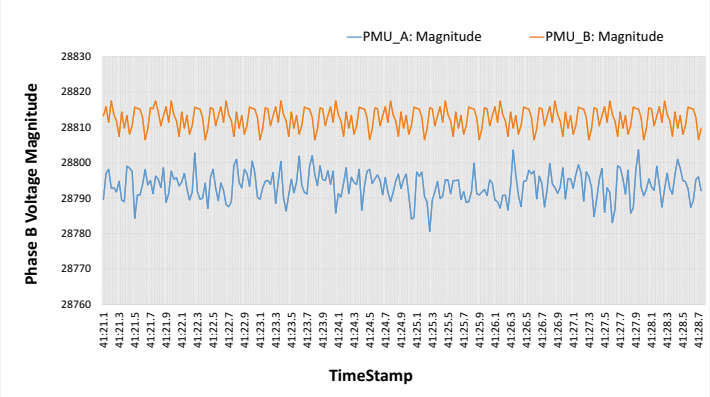

Figure 3.10: Voltage Magnitude Using The Proposed Model

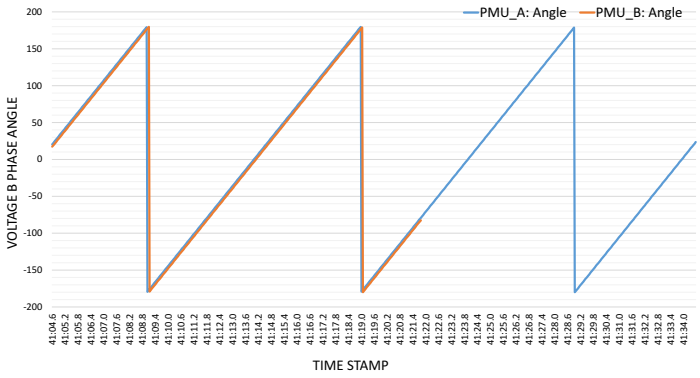

Figure 3.11: Voltage Angle Using The Shortest Path Tree

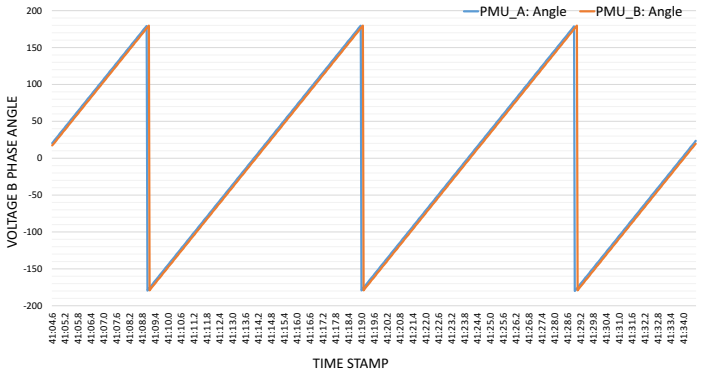

Figure 3.12: Voltage Angle Using The Proposed Model

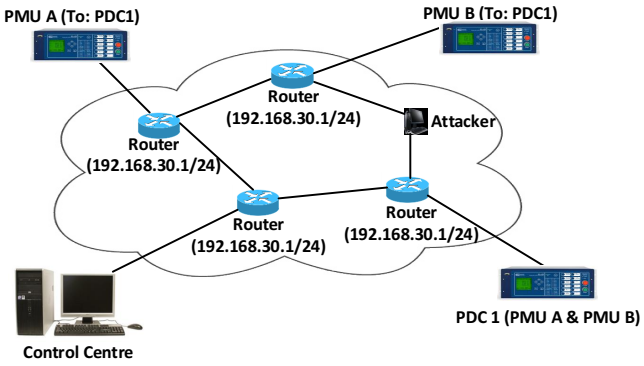

Figure 3.13: Virtual network topology created on openstack

4. Optimal Tree Construction Model for Cyber-Attacks to Wide Area Measurement Systems

4.1 Introduction

Today, the smart grid is being upgraded with the addition of synchrophasor systems,WAMS. They are used to supervise the state of the power grid by collecting measurement values, displayed and processed by human operators and/or control-center applications, from widely distributed sensors. As mentioned in Chapter (2), A common type of sensors is PMUs developed in the early 1980s. PMUs provide a time-stamped voltage and current phasors by utilizing the GPS clock. These time-stamped measurements are then transmitted to a PDC. The role of a PDC is to aggregate and correlate the time-stamped measurements from different PMUs, then sends the correlated measurements to a Super PDC at the control center as shown in Figure (4.1). PMU measurements play an important role in smart grid operations. For instance, solving the system state estimation [104], which is the process of estimating the state of the grid by gathering measurements from geographically dispersed areas through WAMS and SCADA systems. This process is crucial to several applications such as power protection, contingency analysis, corrective actions, real-time

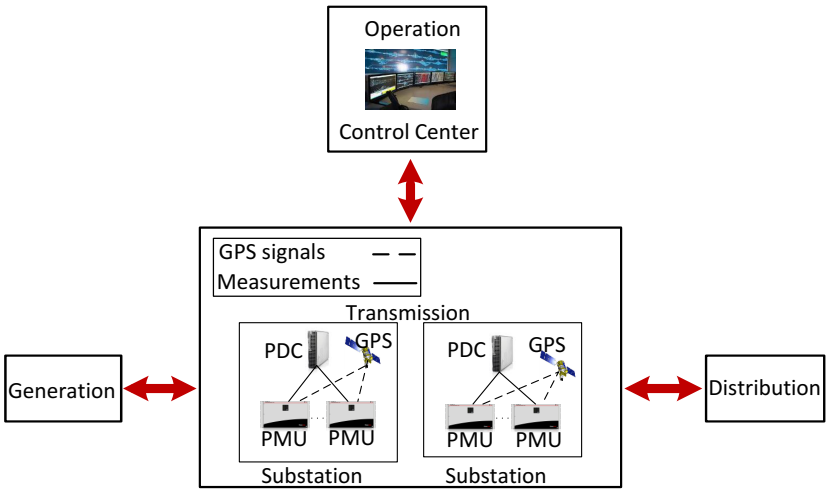

Figure 4.1: WAMS System

pricing, etc. As PMUs are being increasingly deployed, it is predicted that traditional state estimation using conventional measurements from SCADA systems will be ultimately replaced by all-PMU state estimators to enhance the system state estimation and security assessment [21]. However, the increased integration of PMUs introduces new vulnerabilities to cyber-attacks, which if exploited by attackers, may have damaging consequences ranging from local power outage to complete blackout [20, 21]. Therefore, several algorithms have been proposed to detect the presence of such attacks [23–25]. With detection, actions must be considered to prevent the propagation of cyber-attacks, which is the aim of this chapter

As mentioned earlier, it is more reasonable to consider IP Multicast protocols for carrying PMU measurements; IP multicast minimizes packet replication and thus is more bandwidth efficient. The set of nodes that support an IP multicast (the source node, all destination nodes, and all relay nodes) is referred to as a multicast tree. The first node in the PMU multicast tree is called a First-Hop-Router (FHR), which is the first node in the structure between the PMU and its destinations. The multicast tree is updated whenever a

new PDC wishes to become a receiver for a specific PMU; receivers can join and disconnect from the tree at any time [39]. Constructing such multicast trees requires an in-depth knowledge of the WAMS system, which can be available to the system operator. For example, state estimation that runs every few seconds in WAMS gives the system operator direct access to the system state at any given instant, which will provide the operator with a wealth historical data that can be used to characterize the system state [119]. Therefore, several WAMS application can be used to gain the needed knowledge of the system in use.

Now, manipulated PMU measurements received at the control center could result in catastrophic damages to the power grid, especially for applications that rely on PMU measurements for control and protection [38]. Recently, multiple PMU vulnerabilities have been reported by OSlsoft [120]. These vulnerabilities could be exploited remotely causing a data gap for the interface of IEEE C37.118, which is the standard developed to transfer synchropahsor data streams from PMUs to PDCs (see Chapter 2). Therefore, efficient security mechanisms must be implemented to minimize the impact of cyber attacks. Although, the multicast tree proposed in [38] utilizes some security standards such as the IEC 62351, it does not take into consideration the propagation of cyber-attacks. In the presence of an attack, the attacker can use the compromised PMUs to, for instance, propagate the attack to compromise other PMUs and jeopardize the system's observability and reliability. Propagation of cyber-attacks in shared communication network has been studied in other networks [37,85,121,122]. As a relevant instance, worm propagation in mobile ad-hoc networks and metering devices in a secondary distribution network has been studied in [123] and [84], respectively.

Note that under an attack, the system operator will disconnect the compromised detected PMUs from the network [37], which requires Δt time, during such time the attack could propagate to other PMUs to increase the attack damage. In [37], the cyber-attack

propagation in a PMU network is studied and the probability of attack propagation is minimized by disabling detected compromised PMUs and PMUs that are likely to be compromised due to attack propagation. Moreover, the weak authentication and integrity checks and software security of the communication network have been reported in [124].

Under IP multicast, a tree is constructed for each PMU (being its root) to find a path from the PMU to its PDC destinations. The tree may traverse a large number of routers in the network; thus, amplifying the propagation of attacks from a compromised PMU to a set of uncompromised ones along the path to the PDCs. In this context, this chapter addresses the problem of tree construction for collecting PMU measurements while minimizing the impact of the attack propagation from compromised PMUs to others. The relation between the multicast tree of each PMU and the probability of attack propagation has not been addressed before.

This chapter is devoted towards investigating the attack propagation problem in PMUs network; as opposed to existing work [37], here we restrict our attention to the relation between IP multicast and cyber-attack propagation. We propose an optimal IP Multicast tree construction for each connected PMU to minimize the likelihood of cyber-attacks propagation while satisfying the real-time requirements.

4.2 Problem Description

Consider a WAMS that consists of a number of PMUs and PMU data consumers (i.e., PDCs, super PDCs, data historian, etc.) as shown in Figure (4.2). The main components in this system are PMUs, routers, and PDCs. Each PMU is directly connected to a router, through which its measurements are sent to a set of destinations using the IP multicast routing protocol as proposed in [38]. Thus, in this chapter, we consider the problem of gathering PMUs measurements at end paths PDCs using IP multicast forwarding while minimizing cyber attack propagation.

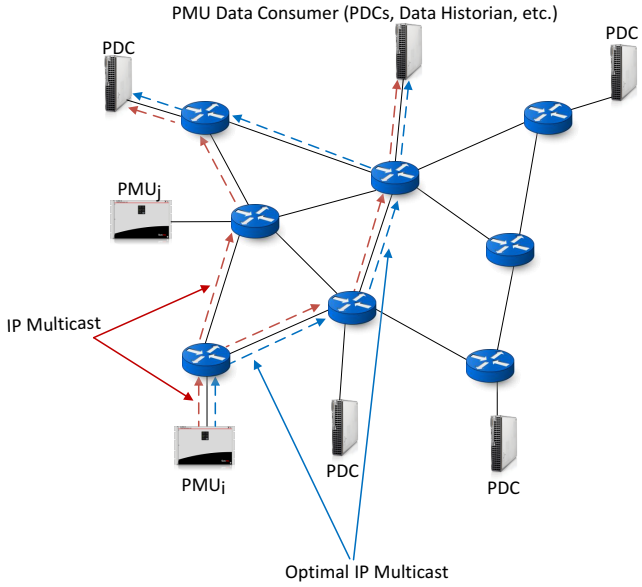

Figure 4.2: PMU Message Stream (IP Multicast)

The system can be abstracted to a directed graph $G = (N, E)$, where E is a set of edges and N is a set of nodes, $N = N_m \cup N_d \cup N_r$, where N_m represents a set of PMUs, where $N_m = \{m_1, \dots m_{|N_m|}\}$. Notion N_d represents a set of PDCs where $N_d = \{d_1, \dots d_{|N_d|}\}$, and N_r is a set of routers connecting PMUs and PDCs where $N_r = \{r_1, \dots, r_{|N_r|}\}$.

Among these nodes, a source $m \in N_m$ sends its measurements to a set of destinations D^m. We assume throughout this chapter that the communication between a source m and its destinations D^m is based on the IP Multicast as proposed in [125]. We also assume that not all routers in the network are connected to PMUs, such routers are considered to be forwarding routers. Hence, let N'_r be a set of routers each is connected to at least one PMU where $N'_r \subseteq N_r$.

In the presence of a cyber-attack, the attacker can use the compromised PMU to propagate the attack to other PMUs through the communication links and the set of routers along the path, which will exacerbate the damage to the power system even further [37].

Namely, and similar to [37], let α_{ij} be the probability that the attack propagates from a compromised PMU$_i$ to an uncompromised PMU$_j$, where $\alpha_{ij} \approx 0$ if PMU$_j$ is not connected

to any router traversed by PMU_i multicast tree. Thus:

$$\alpha_{ij} = \gamma\lambda^{D_{ij}} \tag{4.1}$$

where λ represents the probability that the attack propagates through a router, γ is the probability that the attack propagates to another PMU, and D_{ij} is the number of routers connecting PMU_i and PMU_j, the so-called nodal distance [37].

Our objective in this chapter is therefore to construct multicast trees, each connecting a PMU to its set of PDCs, while minimizing the probability of attack propagation.

4.3 Optimal Tree Construction

In this section, we start with a simple example to illustrate the cyber-attack propagation problem and our proposed multicast tree construction model. Figure (4.3) shows an IEEE 6-bus test system with six buses and eleven transmission lines. To ensure system observability, PMUs are placed at buses 1, 2, 3, 4, and 6 as presented in [37]. Each PMU sends its measurements to a set of destinations (i.e., PDCs, super PDCs, etc.) through a randomly generated data network as shown in Figure (4.3). For instance, if PMU 3 is detected to be under an attack, it takes some time Δt to disconnect the detected compromised PMU, which gives the attack an opportunity to propagate in the network [37]. Therefore, cyber-attack propagation should be considered while constructing the multicast trees to prevent such propagation. A multicast tree of PMU_3 is constructed using our proposed tree construction model and using a shortest path tree construction as shown in Figure (4.4). In the case of shortest path multicast tree, PMU_3 sends the measurements to its FHR (router 4) and follows a shorter path to PDC_1 and PDC_2. Considering PMU_6 (being one of its neighbour) the nodal distance between PMU_3 and PMU_6 is equal to 2, which means that the attack might propagate from PMU_3 to PMU_6 with probability $\alpha_{36} = \gamma\lambda^2$.

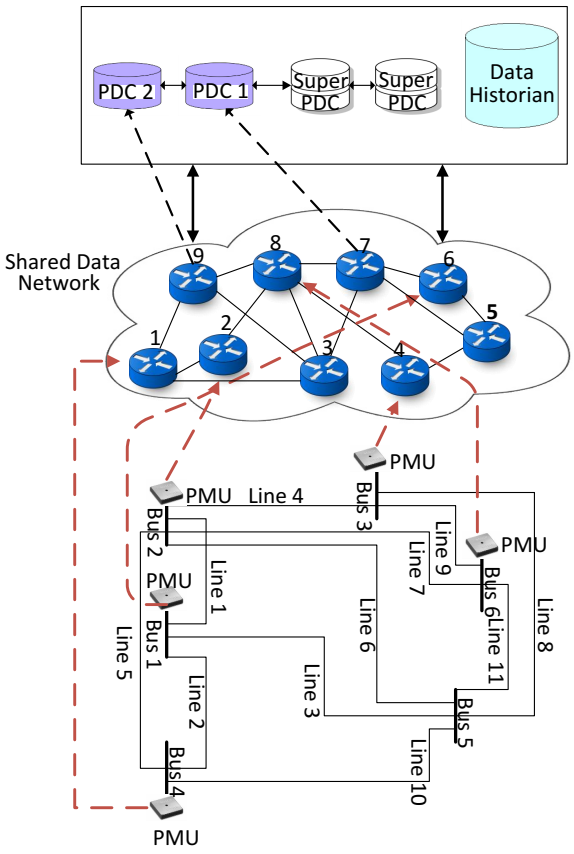

Figure 4.3: 6-Bus Test System

On the other hand, using our proposed tree construction, the multicast tree of PMU_3 follows a longer path (larger nodal distance). In this case, the likelihood that the attack might propagate from PMU_3 to PMU_6 is $\alpha_{36} \approx 0$.

Smart grid applications, which rely on PMU measurements require a fast communication infrastructure that can handle a huge amount of data in near real-time. In such systems, PMUs sample the measured data at an instant known as time tag and then transmit this tagged measurements to PDCs. All measurements with the same time tag should be collected in a timely manner leading to delay requirements in the order of milliseconds [126]. Thus, it is important that the source PMU reaches all terminals within an acceptable delay. The end-to-end delay from a source to a destination can be described as the sum of processing delay, queuing delay, transmission delay, and propagation delay. Processing delay

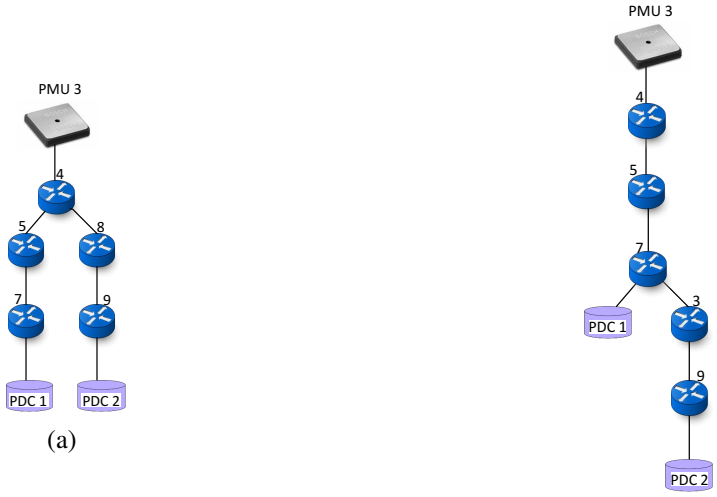

Figure 4.4: PMU_3 Multicast Trees. (a) Shortest Path Tree; (b) Proposed Multicast Tree

can be neglected since routers are considered as forwarding nodes (no processing), measurements processing occurs at end nodes (PDCs) and this processing delay is considered as computation delay not communication delay [102]. Moreover, the propagation delay is assumed to be no more than 1 microsecond [102]. Thus, the total end-to-end communication delay is considered as the sum of transmission delay T_{ij} and queuing delay Q_{ij}, which can be defined as follows:

$$\Delta_{ij} = Q_{ij} + T_{ij}, \quad \forall (i,j) \in E \tag{4.2}$$

Let C_{ij} be the capacity of edge (i,j), f_{ij}^m be the flow from PMU m on edge (i,j), δ_{md} be the delay from PMU m to destination d, and δ_{Th} is a delay threshold (in the range of 100 milliseconds to 5 seconds [102]). Let x_{ij}^m be a binary variable such that:

$$x_{ij}^m = \begin{cases} 1 & \text{if edge } (i,j) \text{ is in the multicast tree of } m \\ 0 & \text{otherwise} \end{cases}$$

Let y_{ij}^{md} be a binary variable such that:

$$y_{ij}^{md} = \begin{cases} 1 & \text{if the path from } m \text{ to } d \text{ traverses edge } (i,j) \\ 0 & \text{otherwise} \end{cases}$$

The queuing and transmission delays can be defined as follows:

$$Q_{ij} = 1 \setminus (\mu - \rho_{ij}), \quad \forall (i,j) \in E \tag{4.3}$$

$$T_{ij} = f_{ij}^{m} \setminus C_{ij}, \quad \forall (i,j) \in E \tag{4.4}$$

where μ is the mean service rate that depends on the port speed and ρ_{ij} is the total traffic through this port on link (i,j), which is the function of the flow conservation variables y_{ij}^{md}. Then, we mathematically formulate the problem of constructing multicast trees with the objective of minimizing the probability of cyber-attack propagation as follows:

4.3.1 Min Attack: to minimize the probability of attack propagation

$$\underset{\mathbf{y,x,f},\alpha,\delta}{\text{Minimize}} \quad \alpha$$

subject to

- *Propagation Probability constraint:*

$$\alpha_{ij} \leq \alpha, \quad \forall i,j \in N_m : i \neq j \tag{4.5}$$

By minimizing α in the objective we are minimizing the probability of attack propagation α_{ij} from a compromised PMU$_i$ to any other connected PMU$_j$, where α is some real number.

- *Flow Conservation Constraints:* to construct our tree we use the following constraints:

$$f_{ij}^{m} - x_{ij}^{m} \geq 0, \quad \forall m \in N_m, (i,j) \in E \tag{4.6}$$

$$x_{ij}^{m} - (f_{ij}^{m}/B) \geq 0, \quad \forall m \in N_m, (i,j) \in E \tag{4.7}$$

$$y_{ij}^{md} \leq x_{ij}^{m} \quad \forall (i,j) \in E, m \in N_m, d \in N_d \tag{4.8}$$

$$\sum_{j:(i,j)\in E} f_{ij}^{m} - \sum_{j:(j,i)\in E} f_{ji}^{m} = \begin{cases} \leq k & \text{if } i = m \\ -1 & \text{if } i = d \\ 0 & \text{if } i = r \end{cases}$$

$$\sum_{j:(i,j)\in E} y_{ij}^{md} - \sum_{j:(j,i)\in E} y_{ji}^{md} = \begin{cases} 1 & \text{if } i = m \\ -1 & \text{if } i = d \\ 0 & \text{if } i = r \end{cases}$$

Constraints (4.6) and (4.7) represent the connectivity between the flow (f_{ij}^{m}) and the tree edges (x_{ij}^{m}), which implies that $f_{ij}^{m} = 0 \Leftrightarrow x_{ij}^{m} = 0$ and $f_{ij}^{m} > 0 \Leftrightarrow x_{ij}^{m} = 1$. Constraint (4.8) indicates that there is no path between m and d along the edge (i,j) unless (i,j) is part of the multicast tree of source m. Finally, the last two constraints describe the flow conservation constraints to ensure that the total incoming flow at a particular node is equal to the total outgoing flow, where k represents the number of all destinations.

- *Subtour Elimination Constraint*: to avoid loops we use the following subtour elimination constraint:

$$\sum_{i \in S} \sum_{j \in S} x_{ij}^{m} \leq |S| - 1, \quad \forall S \subset N, 2 \leq |S| \leq |N| \tag{4.9}$$

- *Edge Capacity Constraint*: to ensure that the constructed multicast tree satisfies edge capacity constraints we use the following constraint:

$$\sum_{m} f_{ij}^{m} \leq C_{ij} \quad \forall (i,j) \in E \tag{4.10}$$

- *Acceptable Delay Constraint*: the following constraint are used to ensure that the constructed multicast tree satisfies the end-to-end delay constraints

$$\delta_{md} = \sum_{(i,j) \in E} y_{ij}^{md} * \Delta_{ij} \quad \forall m \in N_m, d \in D^m \tag{4.11}$$

$$\delta_{md} \leq \delta_{Th} \quad \forall m \in N_m, d \in D^m \tag{4.12}$$

Queuing delay as described in equation (4.3) will yield a non-linear problem formulation since Q_{ij} is modeled as a function of ρ_{ij}. Thus, in this chapter we only consider the transmission delay T_{ij}.

Moreover, calculating the probability in Constraint (4.5) depends on the nodal distance (D_{ij}) between PMU$_i$ and PMU$_j$ as shown in equation (4.1), which varies based on the selected multicast tree; hence, yield a non-linear formulation as well. To overcome this non-linearity, a mathematical transformation can be used where we rewrite the logarithm of the attack propagation ($\log \alpha_{ij} = \log \gamma + D_{ij} \log \lambda$) and instead of minimizing α_{ij}, we equivalently maximize the nodal distance D_{ij}.

Therefore, to tackle the nonlinearity of Constraint (4.5), we cast our problem as a maximization of the nodal distance between PMU$_i$ and PMU$_j$, then we minimize the number of trees traversing a router that is connected to at least one PMU. However,

maximizing the nodal distance between PMUs will expand the multicast tree, leading to an increased delay that might violate the real time requirements for smart grid applications. Therefore, a trade-off between the security level and delay should be considered. Moreover, minimizing the number of incoming links traversing a FHR means that the probability of attack propagation from a router to a PMU will be minimized.

Accordingly, we rewrite our mathematical model to maximize the nodal distance. Let x_j be the number of incoming links (trees) traversing router j where $j \in N'_r$.

4.3.2 Max Nodal Distance:

$$\underset{\mathbf{D,x,h,z}}{\text{Maximize}} \quad \beta$$

Subject to

$$\sum_{i \in N_m, j \in N'_r} D_{ij} - \sum_{j} x_j \geq \beta \quad \forall i, j \in N'_r \tag{4.13}$$

$$x_j = \sum_{m,(i,j) \in E} x_{ij}^m \quad \forall j \in N'_r \tag{4.14}$$

Constraint (4.13) describes the relation between the new objective function, the nodal distance between PMUs, and the number of incoming links to router $j \in N'_r$. Constraint (4.14) presents the number of incoming links traversing a router that is connected to at least one PMU.

Yet, the computation of D_{ij} remains missing. To this extent, we introduce two new binary variable z_{ij}^{mx} and h_{mx} such that:

$$z_{ij}^{mx} = \begin{cases} 1 & \text{if the path from } m \text{ to } x \text{ traverses edge } (i,j) \\ 0 & \text{otherwise} \end{cases}$$

$$h_{mx} = \begin{cases} 1 & \text{if there is a path from } m \text{ to } x \\ 0 & \text{otherwise} \end{cases}$$

Based on this, we can calculate the nodal distance between a source m and any node x as follows:

$$z_{ij}^{mx} \leq x_{ij}^{m} \quad \forall (i,j) \in E, m \in N_m, x \in N_r' \tag{4.15}$$

$$h_{mx} \geq x_{ij}^{m}, \quad \forall m \in N_m, x \in N_r', (i,j) \in E \tag{4.16}$$

$$\sum_{j:(i,j)\in E} z_{ij}^{mx} - \sum_{j:(j,i)\in E} z_{ji}^{mx} = \begin{cases} 1 \times h_{mx} & \text{if } i = m \\ -1 \times h_{mx} & \text{if } i = d \\ 0 & \text{if } i = r \end{cases}$$

$$D_{mx} = \sum_{(i,j)\in E} z_{ij}^{mx} + (1 - h_{mx})B \quad \forall m \in N_m, x \in N_r' \tag{4.17}$$

Constraints (4.15) and (4.16) indicate the relation between z_{ij}^{mx} and x_{ij}^{m}, h_{mx} and x_{ij}^{m}, respectively; where the path from source m to node x traverses edge (i,j) if and only if edge (i,j) is part of m's multicast tree. Constraint (4.3.2) describes the flow conservation constraints of the decision variables z_{ij}^{mx}. The nodal distance between a source m and any node x (D_{mx}) is calculated in constraint (4.17). If x is part of m's multicast tree ($h_{mx} = 1$), then D_{mx} is calculated as presented in constraint (4.17). On the other hand, when $h_{mx} = 0$ (node x is not in the path of m's multicast tree), we set the nodal distance between x and m to a large number B. This number should be as large as the network diameter, to enforce

that m can reach x through a large number of routers. Thus, the propagation becomes less likely since the attack propagation probability decreases exponentially when the distance increases.

Throughout our numerical we solve the following optimization model:

$$\text{Maximize} \quad \beta$$

Subject to

Equations (6) - (20)

4.4 Experimental Results

In this section, we evaluate how well our proposed multicast tree model performs in comparison with a shortest path multicast tree [103]. In these experiments, we consider the IEEE test systems specifically the IEEE 14-bus, IEEE 24-bus, IEEE 30-bus, and IEEE 57-bus along with the New England 39-bus test systems, (interested readers are referred to [127–129]).

Our numerical evaluations are conducted using CPLEX solver version 12.4 on a Windows 7 machine running at 2.67 GHz with 6.00 GB RAM.

The electric power grid is considered completely observable when all of its system states are uniquely identified [104]. The system states can be estimated at the control centre based on the received measurements form sensors across geographically dispersed areas. With the increased deployment of PMUs, a lot of research work has been proposed to find the minimum number of PMUs along with their optimal locations to insure system observability [**?**, 105, 130]. Different scenarios have been studied when finding the optimal PMU placement such as normal conditions, single PMU outages, single branch outages, and with or without conventional measurements. In this chapter, we consider the optimal

Table 4.1: PMU's set of destinations for the IEEE 14-bus (3 destinations)

Bus	Set of destinations
2	$\{d_1, d_2\}$
6	$\{d_1, d_2, d_3\}$
7	$\{d_1, d_3\}$
9	$\{d_1, d_2, d_3\}$

Table 4.2: PMU's set of destinations for the IEEE 24-bus (4 destinations)

Bus	Set of destinations
2	$\{d_1, d_3, d_4\}$
3	$\{d_1, d_2, d_3, d_4\}$
8	$\{d_2, d_3, d_4\}$
10	$\{d_1, d_2\}$
16	$\{d_1, d_3, d_4\}$
21	$\{d_1, d_2, d_3\}$
23	$\{d_1, d_2, d_3, d_4\}$

PMU placement under normal operating conditions with no conventional measurements as presented in [105] and [130]. Table 5.1 shows the optimal number of PMUs needed for observability for each test system and corresponding bus locations. Each PMU sends its measurements to a randomly generated set of destinations as shown in Tables 4.1, 4.2, 4.3, 4.4, and 4.5.

First, we study the probability of attack propagation from each PMU using our proposed tree construction in comparison with the shortest path tree construction. We start by assuming that the attack propagates to another PMU with probability $\gamma = 0.05$, and propagates through a router with probability $\lambda = 0.05$, similar to [37]; our results are shown in Tables 4.7 to 4.12. In all tables, and due to space limits, we only consider PMUs that if compromised, the attack will propagates to other connected PMUs. From the tables, we can see that the proposed multicast tree construction outperforms the shortest path method

Table 4.3: PMU's set of destinations for the IEEE 30-bus (5 destinations)

Bus	Set of destinations
2	$\{d_1, d_4\}$
3	$\{d_2, d_3, d_4, d_5\}$
6	$\{d_1, d_2, d_3\}$
9	$\{d_2, d_4, d_5\}$
10	$\{d_1, d_2, d_3, d_4, d_5\}$
12	$\{d_2, d_5\}$
13	$\{d_1, d_3, d_4, d_5\}$
19	$\{d_2\}$
25	$\{d_1, d_5\}$
27	$\{d_3, d_4, d_5\}$

Table 4.4: PMU's set of destinations for the New England 39-bus (6 destinations)

Bus	Set of destinations
2	$\{d_1, d_2, d_3, d_6\}$
6	$\{d_2, d_4, d_6\}$
9	$\{d_1, d_3\}$
10	$\{d_2, d_3, d_4, d_5, d_6\}$
12	$\{d_1, d_2, d_3, d_4, d_5, d_6\}$
14	$\{d_3, d_4, d_5\}$
17	$\{d_1, d_2, d_5, d_6\}$
19	$\{d_3, d_4\}$
20	$\{d_6\}$
22	$\{d_1, d_3, d_5, d_6\}$
23	$\{d_2, d_4, d_5\}$
25	$\{d_2, d_4\}$
29	$\{d_1, d_3, d_5\}$

Table 4.5: PMU's set of destinations for the IEEE 57-bus (8 destinations)

Bus	Set of destinations
1	$\{d_3, d_5, d_7, d_8\}$
4	$\{d_1, d_2, d_4\}$
6	$\{d_5, d_8\}$
9	$\{d_2, d_3, d_5, d_6, d_7\}$
15	$\{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8\}$
20	$\{d_5, d_7, d_8\}$
24	$\{d_1, d_2, d_3, d_6\}$
25	$\{d_2, d_8\}$
28	$\{d_7\}$
32	$\{d_5, d_6, d_7, d_8\}$
36	$\{d_1, d_2, d_6\}$
38	$\{d_1, d_2, d_4, d_5, d_6, d_7, d_8\}$
41	$\{d_1, d_2, d_4, d_5, d_8\}$
47	$\{d_3, d_4, d_5, d_6, d_7, d_8\}$
50	$\{d_3, d_5, d_8\}$
53	$\{d_1, d_5\}$
57	$\{d_1, d_2, d_5, d_8\}$

Table 4.6: Optimal PMU number and placement for each test system

Test System	Number of PMUs	Bus Locations
IEEE 14-bus	4	2,6,7,9
IEEE 24-bus	7	2,3,8,10,16,21,23
IEEE 30-bus	10	2,3,6,9,10,12,15,19,25,27
New England 39-bus	13	2,6,9,10,12,14,17,19,20,22,23,25,29
IEEE 57-bus	17	1,4,6,9,15,20,24,25,28,32,36,38,41,47,50,53,57

specially for large test systems. We also notice from the tables that for our proposed multicast trees the attack propagates from the compromised PMU to only one connected PMU. While in the shortest path tree construction, the attack propagate from one PMU to more than one PMU, which increase the propagation probability even further. This is due to the fact that increasing the number of compromised PMUs will increase the propagation probability during the same Δt time.

Then, we study the impact of having different values for γ and λ on the attack propagation probability (α_{ij}) in our proposed multicast trees. Again, we consider PMUs that if compromised, the attack might propagate to other connected PMUs, for each test system as shown in Table (4.8). It is clear that increasing the values of γ and λ will increase the attack propagation probability. We observe that in our proposed multicast trees when a PMU is attacked and the probability of attack propagation $\neq 0$ then the nodal distance is always $D_{ij} = 2$; thus, in table 4.8 all results for various values of γ and λ are the same for all PMUs. This is because in our tree construction, the attack propagates from a compromised PMU to a neighbour PMU only when the FHR of the neighbour PMU has a single direct connection to the FHR of the compromised PMU. Thus, the tree path has to traverse the FHR of the compromised PMU in order to reach all its destinations. Since the main objective of our tree construction is to minimize the attack propagation probability, we notice that on all test systems under our proposed model a maximum of one or two PMUs when attacked the attack probability is $\neq 0$.

After that, we study the impact of different attack scenarios on the number of PMUs that are likely to be compromised in the case of cyber-attacks. In the first scenario, we start our experiment by considering a single PMU under attack, then we calculate the percentage of other connected PMUs that are likely to be compromised if this PMU is under attack. We repeat this process for each connected PMU. After that, we calculate the average percentage of all PMUs using our proposed tree construction and the shortest path tree construction as

Table 4.7: Probability of attack propagation (IEEE 14-bus)

Compromised PMU	Method	PMU 1	PMU 3
PMU 2	Shortest Path	1.25×10^{-4}	1.25×10^{-4}
	Proposed Model	1.25×10^{-4}	0
PMU 4	Shortest Path	0	1.25×10^{-4}
	Proposed Model	0	0

Table 4.8: Attack propagation probability with different γ and λ

Compromised PMU	Attack propagation probability α_{ij}						
	$\gamma, \lambda = 0.02$	$\gamma, \lambda = 0.03$	$\gamma, \lambda = 0.04$	$\gamma, \lambda = 0.06$	$\gamma, \lambda = 0.07$	$\gamma, \lambda = 0.08$	$\gamma, \lambda = 0.09$
PMU_2 (14-bus)	8×10^{-6}	2.7×10^{-5}	6.4×10^{-5}	2.16×10^{-4}	3.43×10^{-4}	5.12×10^{-4}	7.29×10^{-4}
PMU_3 (24-bus)	8×10^{-6}	2.7×10^{-5}	6.4×10^{-5}	2.16×10^{-4}	3.43×10^{-4}	5.12×10^{-4}	7.29×10^{-4}
PMU_2 (30-bus)	8×10^{-6}	2.7×10^{-5}	6.4×10^{-5}	2.16×10^{-4}	3.43×10^{-4}	5.12×10^{-4}	7.29×10^{-4}
PMU_5 (30-bus)	8×10^{-6}	2.7×10^{-5}	6.4×10^{-5}	2.16×10^{-4}	3.43×10^{-4}	5.12×10^{-4}	7.29×10^{-4}
PMU_6 (39-bus)	8×10^{-6}	2.7×10^{-5}	6.4×10^{-5}	2.16×10^{-4}	3.43×10^{-4}	5.12×10^{-4}	7.29×10^{-4}
PMU_6 (57-bus)	8×10^{-6}	2.7×10^{-5}	6.4×10^{-5}	2.16×10^{-4}	3.43×10^{-4}	5.12×10^{-4}	7.29×10^{-4}
PMU_7 (57-bus)	8×10^{-6}	2.7×10^{-5}	6.4×10^{-5}	2.16×10^{-4}	3.43×10^{-4}	5.12×10^{-4}	7.29×10^{-4}

Table 4.9: Probability of attack propagation (New England 39-bus)

Compromised PMU	Method	PMU 3	PMU 4	PMU 6	PMU 13
PMU 4	Shortest Path	1.25×10^{-4}	1	0	1.25×10^{-4}
	Proposed Model	0	1	0	0
PMU 5	Shortest Path	6.25×10^{-6}	1.25×10^{-4}	0	6.25×10^{-6}
	Proposed Model	0	0	0	0
PMU 6	Shortest Path	0	0	1	1.25×10^{-4}
	Proposed Model	0	0	1	1.25×10^{-4}
PMU 7	Shortest Path	0	0	1.25×10^{-4}	6.25×10^{-6}
	Proposed Model	0	0	0	0
PMU 8	Shortest Path	0	0	0	6.25×10^{-6}
	Proposed Model	0	0	0	0

shown in Table 4.13. In the second scenario, we consider two PMUs under attack and we calculate the percentage of other PMUs that are likely to be compromised. We repeat this process for each pair of PMUs, then we calculate the average percentage of all PMUs as shown in Table 4.14. It is clear that compromising more PMUs will increase the number

Table 4.10: Probability of attack propagation (IEEE 24-bus)

Compromised PMU	Method	PMU 1	PMU 2	PMU 3	PMU 5	PMU 6	PMU 7
PMU 2	Shortest Path	1.25×10^{-4}	1	1.25×10^{-4}	6.25×10^{-6}	0	0
	Proposed Model	0	1	0	0	0	0
PMU 3	Shortest Path	6.25×10^{-6}	1.25×10^{-4}	1	1.25×10^{-4}	0	0
	Proposed Model	0	0	1	0	1.25×10^{-4}	0
PMU 4	Shortest Path	0	0	0	1.25×10^{-4}	0	0
	Proposed Model	0	0	0	0	0	0
PMU 5	Shortest Path	3.125×10^{-7}	6.25×10^{-6}	1.25×10^{-4}	1	0	0
	Proposed Model	0	0	0	1	0	0
PMU 6	Shortest Path	0	0	0	0	1	6.25×10^{-6}
	Proposed Model	0	0	0	0	1	0

Table 4.11: Probability of attack propagation (IEEE 30-bus)

Compromised PMU	Method	PMU 1	PMU 2	PMU 3	PMU 4	PMU 6	PMU 7	PMU 9
PMU 2	Shortest Path	1.25×10^{-4}	1	1.25×10^{-4}	0	0	3.125×10^{-7}	1.57×10^{-8}
	Proposed Model	0	1	1.25×10^{-4}	0	0	0	0
PMU 3	Shortest Path	6.25×10^{-6}	1.25×10^{-4}	1	0	0	0	0
	Proposed Model	0	0	1	0	0	0	0
PMU 4	Shortest Path	0	0	0	1	0	1.25×10^{-4}	6.25×10^{-6}
	Proposed Model	0	0	0	1	0	0	0
PMU 5	Shortest Path	3.125×10^{-7}	6.25×10^{-6}	1.25×10^{-4}	1.25×10^{-4}	0	6.25×10^{-6}	3.125×10^{-7}
	Proposed Model	0	0	1.25×10^{-4}	0	0	0	0
PMU 6	Shortest Path	0	0	0	0	1	0	1.25×10^{-4}
	Proposed Model	0	0	0	0	1	0	0
PMU 7	Shortest Path	0	0	0	0	0	1	1.25×10^{-4}
	Proposed Model	0	0	0	0	0	1	0
PMU 9	Shortest Path	0	0	0	0	1.25×10^{-4}	0	1
	Proposed Model	0	0	0	0	0	0	1
PMU 10	Shortest Path	0	0	0	0	6.25×10^{-6}	0	1.25×10^{-4}
	Proposed Model	0	0	0	0	0	0	0

of other connected PMUs that are likely to be compromised. This is because attacking more PMUs increases the propagation of the attack during the same Δt time, as discussed earlier. From Tables 4.13 and 4.14, we can see that the propagation of the attack and the size of the system has an inverse relationship as the probability decreases when the network size increases for both multicast trees; however, our tree construction still outperforms the shortest path with lower attack propagation probability.

Table 4.12: Probability of attack propagation (IEEE 57-bus)

Compromised PMU	Method	PMU 1	PMU 2	PMU 8	PMU 9	PMU 11	PMU 13	PMU 15	PMU 16	PMU 17
PMU 1	Shortest Path	0	1.25×10^{-4}	0	0	0	0	0	0	0
	Proposed Model	0	0	0	0	0	0	0	0	0
PMU 2	Shortest Path	1.25×10^{-4}	0	0	0	0	0	0	0	0
	Proposed Model	0	0	0	0	0	0	0	0	0
PMU 6	Shortest Path	0	0	0	0	0	0	0	1.25×10^{-4}	0
	Proposed Model	0	0	0	0	0	0	0	0	1.25×10^{-4}
PMU 7	Shortest Path	0	0	6.25×10^{-6}	0	0	0	0	0	1.25×10^{-4}
	Proposed Model	0	0	0	0	0	0	0	0	1.25×10^{-4}
PMU 10	Shortest Path	0	0	0	1.25×10^{-4}	0	0	0	0	0
	Proposed Model	0	0	0	0	0	0	0	0	0
PMU 11	Shortest Path	0	0	0	0	0	1.25×10^{-4}	0	0	0
	Proposed Model	0	0	0	0	0	0	0	0	0
PMU 12	Shortest Path	0	0	0	0	1.25×10^{-4}	6.25×10^{-6}	0	0	0
	Proposed Model	0	0	0	0	0	0	0	0	0
PMU 14	Shortest Path	0	0	0	0	0	0	1.25×10^{-4}	0	0
	Proposed Model	0	0	0	0	0	0	0	0	0
PMU 15	Shortest Path	0	0	0	0	0	0	0	1.25×10^{-4}	0
	Proposed Model	0	0	0	0	0	0	0	0	0

Table 4.13: Average % of PMUs that are likely to be compromised (with one initially compromised PMU)

Model	IEEE 14-bus	IEEE 24-bus	IEEE 30-bus	New England 39-bus	IEEE 57-bus
Shortest Path	19%	22%	19%	5%	4%
Proposed Model	6%	2%	2%	1%	1%

Then, we compare the computational time of our proposed tree construction in each test system as shown in Table 4.15. It is clear that the run time of our trees is relatively small. In particular, in the 57-bus test system, the time needed to construct the 17 multicast trees is less than 4 seconds. This shows that our tree construction method is quite scalable for larger systems. We nonetheless believe that efficient tree construction methods for larger WAMS systems, while considering cyber attacks, using efficient heuristics could be subject for further investigation, which currently is outside the scope of this work.

Finally, we note that, as discussed earlier, the objective of our tree model is to minimize the probability of attack propagation, which can be done by maximizing the nodal distance

Table 4.14: Average % of PMUs that are likely to be compromised (with two initially compromised PMU)

Model	IEEE 14-bus	IEEE 24-bus	IEEE 30-bus	New England 39-bus	IEEE 57-bus
Shortest Path	30%	38%	31%	9%	8%
Proposed Model	11%	4%	4%	1%	1%

Table 4.15: CPU run-time using the proposed tree construction

IEEE 14-bus	IEEE 14-bus	IEEE 14-bus	New England 39-bus	IEEE 57-bus
.95 seconds	.98 seconds	1.22 seconds	2.67 seconds	3.56 seconds

between PMUs while satisfying real-time requirements. Even though our proposed multi-cast trees did not eliminate the attack propagation completely, our model outperform, with lower propagation probability, the shortest path tree specially for large test systems.

5. A Power System Observability-Based Recovery Scheme for WAMS Phasor Data Collection

5.1 Introduction

As mentioned in Chapter (1), today's smart grid tightly connects the power generation, transmission, distribution, and consumption using advanced IT technologies to provide reliable, resilient, and cost-efficient energy services. However, due to the increase in power demand, modern transmission power systems are often operating close to their stability limits causing several disturbances and power outages [131]. This has increased the importance of implementing suitable and efficient techniques for analyzing, monitoring, predicting, and quickly recovering possible disturbances in the system. As a consequence, there is a need for a technology that facilitates the understanding and management of the increasingly complex behaviour exhibited by large power systems. Therefore, a new technology for real-time monitoring, control, and protection through synchronized phasor measurements is proposed. Such technology allows the grid monitoring and control to be adjusted depending on the evolution of events in real-time, which involves the use of PMU, PDC, communication technologies, and applications that rely on synchrophasor measurements.

These measurements are synchronized with the time signal of a Global Positioning System (GPS) with a sampling rate in the order of milliseconds, which gives adequate tools to monitor, control, and protect the smart grid in a wide geographical area. One of the benefiting applications of such technology is state estimation application that estimates the state of the grid based on real-time synchrophasors. An accurate and secure estimate of the grid is of great importance for several applications such as power protection, contingency analysis, voltage stability, real-time pricing, etc. Therefore, the availability of synchrophasor is crucial to the system observability and the estimation process. A system is said to be observable if based on the received measurements the system state can be estimated.

5.1.1 State Estimation

The power system state estimation has been proposed since the sixties. Prof Schweppe, the leading researcher of the Power System Engineering Group at MIT, was the first to develop the idea of state estimation for power system monitoring. State estimation is used in system monitoring to best estimate the grid through the analysis of the received measurements. The state estimation is designed to handle uncertainties using measurement readings with an actual system in real time [132]. These uncertainties are due to communication errors, incomplete measurements, unexpected system changes, etc. The goal of the estimator is to ”clean up” the input data and provide a reliable set of state estimates to the control center that truly represent the actual system states.

The state estimation uses power flow models, which is a set of equations that describe the energy flow on transmission lines. An Alternate Current (AC) power flow model is a power flow model that consists of both a real and a reactive power flow model. AC power flow can be represented using non-linear equations, which is computationally expensive to solve in many cases for large power systems. Thus, power system engineers often consider the Direct Current (DC) power flow model, which considers only the real power and can be

represented using linear formulation. Although the DC power flow model is less accurate than the AC power flow model, the DC model is simpler than the AC model [28].

The state estimators are generally based on a weighted least-squares cost criterion [132], which has a long history of successful applications in many fields. However, this criterion is very sensitive to bad data, which may cause poor estimates. Consequently, power system researchers proposed Bad Data Detection (BDD) algorithms to detect the presence of such bad data.

The estimation process is solved iteratively using weighted least squares estimator (WLS), which is a widely used and well-investigated method. WLS estimator is non-robust in the presence of bad measurements; thus, a bad data processor to detect, identify, and correct any existing bad data should be carried out. Here, we present a common formulation of the state estimation problem under DC power flow model.

$$z = Hx + e \tag{5.1}$$

where $H \in R^{M*N}$ is the dc power flow matrix, $z \in R^M, x \in R^N$, and $e \in R^M$ are the sensor measurements vector, the system state vector, and the measurements noise vector, respectively. Moreover, Hx is a vector of m linear functions linking measurements to states, where we have m measurements and n state variables.

With the increased deployment of PMUs, conventional state estimators are assumed to be replaced with all-PMU state estimator [21] due to their optimal deployment and utilization for a wide variety of power system control applications. Much research interest has been developed to propose and enhance the conventional state estimation process to utilize the phasor measurements. In [133], an estimation algorithm based on alternating minimization and parallel Kalman filtering using PMUs with phase mismatch has been proposed. The authors in [134] enhanced the classical state estimation to utilize synchronized phasor measurements in a non-invasive fashion.

As mentioned earlier, WLS is a well-known and widely used method for state estimation. This algorithm is iterative when conventional measurements are used; however, it can be simplified and non-iterative when only PMU measurements are used. The measurement and WLS estimation equations will take the following form:

$$\hat{x} = (H^T W H)^{-1} H^T W z \tag{5.2}$$

where W is a diagonal matrix whose elements are the measurements wights.

To ensure the system observability, enough measurements should arrive at the estimator to make the state estimation process possible. The minimum set of measurements needed to estimate the n state variables is commonly called basic measurements, and the remaining measurements are referred to as redundant measurements [23]. However, observability tests can be carried out based on the properties of the measurements Jacobian H. If the Jacobian has full column rank, then the system will be considered fully observable. Note that for dc estimators, any set of n measurements whose corresponding rows in H are linearly independent are sufficient to solve the n state variables, which means that it contains the set of basic measurements. That is, n independent linear equations are sufficient to solve for n variables. In other words, the rank of H should be equal to n, which means that at least n rows of H are linearly independent vectors. These rows should correspond to at least one set of the basic measurements. Note that the choice of a set of basic measurements is not unique, multiple sets of basic measurements exist [23]. Finding the set of basic measurements has been addressed in many research work including [135–137]. A straight forward but brute force approach is to randomly choose a set of n measurements out of m and see if the rows corresponding to them in H are linearly independent [23].

In general, WAMS requires more information to be transmitted and processed to improve the grid efficiency [138]. However, the wide use of communication networks creates more vulnerabilities to cyber-attacks. Such attacks are especially harmful if, as a consequence,

physical damages are made on the power quality and devices. Therefore, the security of WAMS is a key factor in smart grid technology, since errors of monitoring measurements introduced by malicious attackers will cause wrong decisions, which may lead to catastrophic consequences. A multitude of security threats targeting WAMS such as false data injection attack, DoS, man-in-the-middle, and replay attack has been discussed in the literature. For example, inaccuracies in the state information arising from cyber-attacks can result in a severe degradation of the grid's performance, affect accurate predictions of transmission status, and result in delays in the mitigation of power network failures.

Even though WAMS communication network tends to be a dedicated Intranet, this does not mean that such networks are immune to cyber-attacks. For instance, removable media such as USB drives can be used to carry malware, and hack computers for later use as attack sources. Moreover, a large number of mobile devices can be used as a malicious medium, and we cannot rule out the possibility that utility employees directly attack the network [8, 106]. More importantly, regardless of the causes, the impacts of acting on incorrect or missing information will have already propagated into the rest of the system. At this stage, it may already be too late to avoid a wide-area power outage within the grid [106].

As PMUs and PDCs are connected via an IP-based network where malware at a compromised PMU or PDC can infect other devices through network connections [122, 139]. Consequently, upon detection of attacks, compromised PMU or PDCs should be disconnected from the communication network to avoid cyber-attack propagation as suggested by NIST [140]. Although the disconnection of compromised PMUs or PDCs can prevent further propagation of the attack, the traffic initiated from those devices can no longer reach WAMS applications. As a result to this disconnection, the system observability can be significantly reduced as the estimation process can not be performed based on the received synchrophasors; hence, affect other WAMS applications.

Figure (5.1) shows an illustrative example where two PDCs are receiving measurements from different PMUs. One PDC (PDC1) is detected to be under attack. To prevent the attack propagation PDC1 is disconnected from the network, which means losing measurements from (PMU1 and PMU2) even though both PMUs can send trusted measurements. Losing some PMU measurements might have an impact on the system observability; thus to maintain the observability some measurements need to be re-routed to other connected PDC (PDC 2). However, such process needs to take into consideration WAMS functional requirements such as end-to-end delay from the PMU to the new PDC and the value of the PDC timer. As straightforward rerouting may violate the end-to-end delay, or cause a measurement drop due to the expiration of the PDC timer. Moreover, this rerouting should consider the possible impact on other connected PMUs (PMU3, PMU4, and PMU5).

Based on the above-mentioned challenges, the contribution of this chapter is to mitigate the impact of attacks on PDCs in a timely manner. We investigate the rerouting process of un-compromised PMUs (after disconnecting a compromised PDC) to other connected un-compromised PDCs after attacks while considering delay and timer requirements. Such rerouting ensure system observability, and prevent consequences of the loss of PMU measurements. The presented approach is formulated as a linear program taking into consideration the functionality constraints of WAMS network, and the use of PMU measurements in system observability.

5.2 System Model

In general, WAMS applications rely on synchrophasor from remote measurement devices at substations and in the field. synchrophasor measurements are communicated back to the control centre/application through an IP-based network using a variety of protocols and communication media such as the IEEE C37.118 [141] and the IEC 61850-90-5 [142].

As mentioned previously in Chapter (2), the PDC groups measurements from different

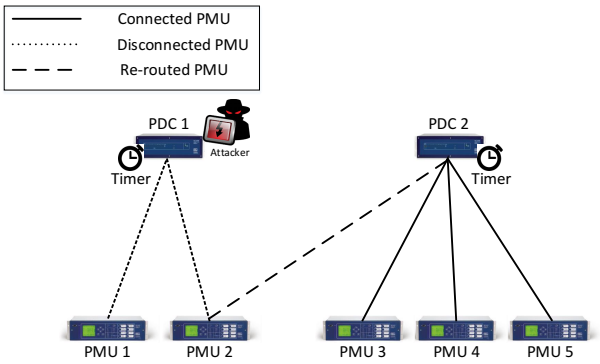

Figure 5.1: An Illustrative Example

PMUs with the same time stamp into a time-stamped buffer. A timer per time-stamped buffer is added. The countdown of the timer starts when the first measurement with a new time stamp arrives at the PDC. Then, the PDC assigns a new buffer to this newly arrived measurement and starts the timer. When the timer goes off, the PDC forwards the received measurements without waiting for the entire measurements to arrive. In case of delays, this wait time ensures that the PDC forwards the phasor measurements in an acceptable time range without waiting for the delayed measurements to arrive. However, this timer introduces the issue of data incompleteness when synchrophasor measurements arrive after the expiration of the PDC timer are dropped at the PDC [30].

5.2.1 Problem Description

To achieve the goals of WAMS, from a communication network perspective, measurements from PMUs should be securely sent and delivered to PDCs and the control centre. From physical system perspective, PMUs installed in different parts of the grid should ensure the observability of the whole system in real-time, so that state estimation and other

advanced power system applications can be performed.

After a detection of a cyber-attack targeting PDCs, the compromised PDCs are disconnected from the network to avoid the propagation of cyber-attack to other connected nodes in the network. Although this disconnection helps in minimizing the attack propagation, it degrades the system observability. Simply because disconnecting a PDC means disconnecting all PMUs sending to that PDC, even though they might not be compromised; hence, the received measurements at the control system might not be enough to ensure system observability. Thus, a fast mitigation of the impact of such an attack needs to be considered and the disconnected un-compromised PMUs need to be re-routed to other PDCs to maintain the system observability. Therefore, in this chapter, we propose a mathematical model to re-route disconnected and un-compromised PMUs to other PDCs to maintain the system observability. As opposed to existing work [89], we consider the end-to-end delay and PDC timer during the re-routing process.

System Observability

A system is said to be observable if, based on the received synchrophasor measurements, we get enough information to determine the state of the system in real-time. When a PMU is installed at a bus, the voltage phasor at that bus and current phasor of all branches connected to it can be measured.

In general, the observability function of a bus $m \in B$ is defined as a function of the PMU location [89] :

$$O_m = \sum_{n \in N_u} a_{mn} x_n \tag{5.3}$$

where B is a set of buses and x_n is a binary variable such that:

$$x_n = \begin{cases} 1 & \text{if a PMU is installed at bus } n \\ 0 & \text{otherwise} \end{cases}$$

and a_{mn} is the connectivity parameter, defined as:

$$a_{mn} = \begin{cases} 1 & \text{if } m = n \text{or } (m,n) \in L \\ 0 & \text{otherwise} \end{cases}$$

where L is a set of transmission lines and $O_m \geq 1$ implies that bus m is observable, as the voltage phasor at bus m can be either measured by the PMU at bus m, or be calculated by PMUs at neighbours of bus m. The power system is said to be observable if the observability function O_m for each bus is greater than or equal to 1:

$$O_m \geq 1, \quad \forall m \in B \tag{5.4}$$

With the disconnection of some PDCs due to cyber-attacks, the observability function O_m at some buses may become 0; thus, the system is no longer observable. However, it is possible to reconnect some disconnected yet un-compromised PMUs to the communication network to restore the system observability. During the process of reconnecting un-compromised PMUs, the timer of each PDC and the end-to-end delay need to be considered. Moreover, this process should not have an impact on other connected PMUs.

5.2.2 Problem Definition

Consider a distributed WAMS with a set of PMUs $N_u = \{u_1, ..., u_{|N_u|}\}$ and a set of PDCs $N_c = \{c_1, ..., c_{|N_c|}\}$.

The system can be abstracted to a directed graph $G_c = (N, E)$, where E is a set of edges (communication lines) and N is a set of nodes such that $N = N_u \cup N_c \cup N_r$. The notion

N_r represents a set of routers connecting PMUs and PDCs where $N_r = \{r_1, \ldots, r_{|N_r|}\}$.

Each PDC c receives synchrophasor measurements from a set of PMUs. Let $U_c = \{u_i\}_{x_{ic}=1}$ be the set of PMUs sending their measurements to PDC c, where x_{ic} is equal to one when PMU i sends measurements to PDC c.

On the other hand, we consider a power transmission network abstracted as a graph $G_p(B, L)$, where B denotes the set of buses and L denotes the set of transmission lines. We assume that PMUs are installed in different part of the grid to ensure system observability [105]. Let N_u be the set of buses where PMUs are installed where $N_u \subseteq B$.

After the disconnection of PDCs as response to cyber-attack, we check the observability function at each bus m. Depending on the system observability, we either wait for the compromised PDCs to be fixed or consider solving the following problem to recover the system observability and find the best route to connect PMUs with PDCs such that equation (5.4) satisfies.

Let $\bar{c}$ be the compromised detected PDC that has been disconnected from the network to avoid cyber-attack propagation and $U_{\bar{c}} = \{u_i\}_{x_{u_i\bar{c}}=1}$ be the set of PMUs sending to PDC $\bar{c}$.

If a PDC is disconnected then measurements from all PMUs sending to this PDC will be lost and O_m might not be equal to one for all buses. In this case, we need to find the minimum number of the disconnected PMUs $u_i \in U_{\bar{c}}$ to be rerouted such that $O_m \geq 1$ for all buses.

Let y_{uc} and y_{ij}^{uc} be binary variables such that:

$$y_{uc} = \begin{cases} 1 & \text{if a disconnected un-compromised measurement from } u \in U_{\bar{c}} \text{is rerouted to PDC} c \\ 0 & \text{otherwise} \end{cases}$$

$$y_{ij}^{uc} = \begin{cases} 1 & \text{if the path from } u\text{to}c\text{travers link}(i,j) \\ 0 & \text{otherwise} \end{cases}$$

Therefore, the objective function of the proposed model is to reroute the least number of measurements from disconnected PMUs that can improve the system observability. This objective can be represented as follows:

$$\text{Minimize} \sum_{u \in U_{\bar{c}}} \sum_{c \in N_c \setminus \{\bar{c}\}} y_{uc}$$

Subject to

- *System observability*: this constraint ensures that the new re-routed measurements maintain the system observability by checking the observability function O_m for each bus $m \in B$.

$$O_m \geq 1, \quad \forall m \in B \tag{5.5}$$

$$O_m = \sum_{n \in N_u} a_{mn} \cdot x_n \cdot \sum_{c} y_{nc} \geq 1 \quad \forall m \in B \tag{5.6}$$

- *PDC timer and end-to-end delay constraints:* a measurement $u \in U_{\bar{c}}$ can be re-routed to PDC c if its end-to-end delay δ_{uc} (from the source PMU to the destination PDC) is less than a specified threshold (δ_{Th}), and if it arrives at the PDC within an acceptable time window (defined by the timer which is initiated when a PMU measurement with a new time stamp arrives first); this can be translated mathematically as follows:

$$\delta_{uc} \leq \delta_{Th} \tag{5.7}$$

$$\delta_{uc} \leq \delta_{u^*c} + t_{out} \tag{5.8}$$

where t_{out} is the PDC timer, and δ_{u^*c} is the delay of the *first* received measurements with a new time stamp. In other words, $\delta_{u^*c} = \min_{u}(\delta_{uc})$. Knowing the time of the first received measurement, and the timer length for a PDC is useful for calculating the number of received measurements within a timeout period as described in equation (5.8). To write δ_{u^*c} expression as a minimum into a Linear Program format, we introduce the following variables. Let $x^c_{uu'}$ and x'_{uc} be binary variables such that:

$$x^c_{uu'} = \begin{cases} 0 & \text{if} \delta_{uc} \leq \delta_{u'c} + t_{out} \\ 1 & \text{otherwise} \end{cases}$$

$$x'_{uc} = \begin{cases} 0 & \text{if } \sum_{u' \neq u} x^c_{uu'} = 0 \\ 1 & \text{if } \sum_{u' \neq u} x^c_{uu'} > 0 \end{cases}$$

$$\delta_{uc} \leq \delta_{u'c} + t_{out} + x^c_{uu'} \times M, \quad \forall u \in N_u, c \in N_c \backslash \{\bar{c}\}, u' \in N_u, u \neq u' \tag{5.9}$$

$$\delta_{uc} \geq \delta_{u'c} + t_{out} - (1 - x^c_{uu'})M, \quad \forall u \in N_u, c \in N_c \backslash \{\bar{c}\}, u' \in N_u, u \neq u' \tag{5.10}$$

Constraints (5.9) and (5.10) are the linearization of the decision variable $x^c_{uu'}$, where $\delta_{u'c}$ is the delay from all PMUs (u') to PDC (c).

$$\sum_{u' \neq u} x^{c}_{uu'} > x'_{uc} - 1, \quad \forall u \in N_u, c \in N_c \backslash \{\bar{c}\} \tag{5.11}$$

$$\sum_{u' \neq u} x^{c}_{uu'} \leq x'_{uc} \times M, \quad \forall u \in N_u, c \in N_c \backslash \{\bar{c}\} \tag{5.12}$$

$$\sum_{u' \neq u} x^{c}_{uu'} \geq 0, \quad \forall u \in N_u, c \in N_c \backslash \{\bar{c}\} \tag{5.13}$$

Constraints (5.11), (5.12), and (5.13) specify that when the measurement (u) arrives within c's timer, then the value of x'_{uc} should be equal to zero.

The end-to-end communication delay from a source to a destination can be described as the sum of processing delay, queuing delay, transmission delay, and propagation delay on each link along the path connecting the source (PMU) and destination (PDC). Processing delay can be neglected since routers are considered as forwarding nodes (no processing), measurements processing occurs at end nodes (PDCs) [102]. Moreover, the propagation delay is assumed to be no more than 1 microsecond [102]. Thus, each link (i, j) along the path experiences a delay Δ_{ij} computed as follows:

$$\Delta_{ij} = t^{ij}_{trans} + t^{ij}_{que} + t^{ij}_{prop} \tag{5.14}$$

where t^{ij}_{trans} and t^{ij}_{que} are the transmission delays and queuing delays on link (i, j) respectively. The transmission delay t^{ij}_{trans} on (i, j) is calculated as follows:

$$t^{ij}_{trans} = f_{ij}/C_{ij}, \quad \forall (i, j) \in E \tag{5.15}$$

where f_{ij} is the total flow (e.g., number of packets carrying measurements) on link (i, j) that can be calculated as follows:

$$f_{ij} = \sum_{u \in N_u - U_{\bar{c}}} f_{ij}^u + \sum_{u \in U_{\bar{c}}} f_{ij}^u, \quad \forall (i,j) \in E \tag{5.16}$$

where f_{ij}^u is the flow from PMU u on link (i,j).

The queuing delay (of packets at node i which are forwarded on link (i,j) can be determined by the traffic behaviour and can be approximated as follows:

$$t_{que}^{ij} = 1/(\mu - \rho_{ij}), \quad \forall (i,j) \in E \tag{5.17}$$

where μ is the mean service rate (e.g., average number of packets processed per second by the router) which depends on the port speed and ρ_{ij} is the average rate of traffic arriving to this port; ρ_{ij} is modelled as a function of the flow conservation variables y_{ij}^{uc}. Finally, the propagation delay t_{prop}^{ij} is calculated by the distance between nodes and the speed of light in the communication medium.

Now, the end-to-end delay can be calculated as follows:

$$\delta_{uc} = \sum_{(i,j) \in E} y_{ij}^{uc} * \Delta_{trans}^{ij}, \quad \forall c \in N_c \backslash \{\bar{c}\}, u \in N_u \tag{5.18}$$

- *Flow Conservation Constraints:* to deliver measurements between PMUs and PDCs we use the following constraints:

$$\sum_{j:(i,j) \in E} y_{ij}^{uc} - \sum_{j:(j,i) \in E} y_{ji}^{uc} = \begin{cases} y_{uc} & \text{if } i = u \quad \forall u \in U_{\bar{c}} \\ -y_{uc} & \text{if} i = c \quad \forall c \in N_c \backslash \{\bar{c}\} \\ 0 & \text{if} i = r \quad \forall r \in N_r \end{cases}$$

$$f_{ij}^u \leq \sum_{c \backslash \{\bar{c}\}} y_{ij}^{uc} \quad \forall u \in U_{\bar{c}}, (i,j) \in E \tag{5.19}$$

$$f_{ij}^{u} \geq y_{ij}^{uc} \quad \forall u \in U_{\bar{c}}, c \in N_c \backslash \{\bar{c}\}, (i,j) \in E \tag{5.20}$$

The first Constraint represents the flow conservation constraints for y_{ij}^{uc}. Constraints (5.19) and (5.20) describe the relation between y_{ij}^{uc} and f_{ij}^{u} as if link (i,j) is on the path from u to c, then this link should have flow from PMU u.

- *Edge Capacity Constraint*: to ensure that the constructed tree satisfies edge capacity constraints we use the following constraint:

$$f_{ij} \leq C_{ij}, \quad \forall (i,j) \in E \tag{5.21}$$

- *One PDC is selected for each PMU*: this constraint ensure that PMU $u \in U_{\bar{c}}$ is sending to at most one PDC c.

$$\sum_{c \in N_c - \{\bar{c}\}} y_{uc} \leq 1, \quad \forall u \in U_{\bar{c}} \tag{5.22}$$

$$y_{uc} \geq y_{ij}^{uc} \quad \forall (i,j) \in E, u \in U_{\bar{c}}, c \in N_c \backslash \{\bar{c}\} \tag{5.23}$$

5.3 Numerical Results

To evaluate the proposed approach, and its usefulness in maintaining system observability, we implemented the developed model and related simulation programs using Java and IBM CPLEX concert technology. The simulations were executed on a windows machine with Intel Core i7 CPU running at 2.67GHz and equipped with 6 GB of RAM. We tested our approach on the 14-bus, 24-bus, and 30-bus IEEE test systems (for details about those systems, interested readers are referred to [127–129]), and compared the collected results with the approach presented in [89]. Moreover, our numerical results are contrasted to

those of a base method that re-routes measurements from disconnected PMUs to available PDCs to maintain system observability.

In our system setup, we consider the electric grid to be observable when all of its system states are uniquely identified [104]. Those states can be estimated at the control center based on the measurements received from sensors dispersed across the grid. This is made possible through the deployment of PMUs at optimal bus locations in the grid as presented by [105]. We adopt the results of [105] for PMU placement under normal operating conditions with no conventional measurements for system observability. The optimal number of PMUs for each test system is presented in Table 5.1 along with the corresponding bus locations. Each of those PMUs sends its measurements to a randomly selected set of PDCs with sampling rate up to 60 samples/second. The synchrophasor sampling rate varies depending on the application. For example, control applications require high sampling rate up to 120 samples/second while some monitoring application such as the state estimation requires 30-60 samples/second [143]. The bandwidth considered in this set up is 2-5 Mbits/s for applications with low to medium data rate [109]. We also consider packet size of 128 bytes similar to what has been proposed in [12]. Moreover, the communication links are placed in parallel with the transmission lines and each bus is represented as a communication node which can send, receive and route measurements [80]. For a detailed model of realistic communication for the IEEE 14-bus standard test system readers are refereed to [108].

We conducted two sets of experiments to analyze the usefulness of our approach in mitigating the impact of cyber attacks on PDCs. The first set of experiments presume the deployment of the optimal number of PMUs only at the locations identified in Table 5.1. Under this assumption, we consider attacks targeting a single PDC at a time and then multiple PDCs, and report on the ability of the compared approaches to fulfill system observability. In the second set of experiments, we add redundant PMUs into each test system, and evaluate the impact of the compared approaches in restoring system observability in

Table 5.1: Optimal PMU number and placement for each test system

Test System	Number of PMUs	Bus Locations
IEEE 14-bus	4	2,6,7,9
IEEE 24-bus	7	2,3,8,10,16,21,23
IEEE 30-bus	10	2,3,6,9,10,12,15,19,25,27

the presence of single and multiple PDC failures. The PMU to PDC connectivity for IEEE 14-Bus, 24-Bus and 30-Bus systems, under optimal PMU placement and in the presence of redundant PMUs, is presented in Tables 5.2, 5.3, and 5.4 respectively where we identify each PMU by its respective bus location. Those tables are based on results collected from our previous work [143] that establishes multicast trees for PMUs in the WAMS communication network.

Table 5.2: PMU to PDC Connectivity - 14 Bus System

PMU / PDC	Optimal				Redundant	
	2	6	7	9	10	13
1	✓		✓			
2		✓			✓	
3				✓		✓

Table 5.3: PMU to PDC Connectivity - 24 Bus System

PMU / PDC	Optimal							Redundant		
	2	3	8	10	16	21	23	11	12	17
1	✓		✓							✓
2		✓			✓				✓	
3				✓			✓			
4						✓		✓		

5.3.1 Optimal PMU placement for system observability:

In this subsection, we consider the minimum number of PMUs to ensure system observability as proposed in [105]. Each PMU sends its measurement to a destination PDC

Table 5.4: PMU to PDC Connectivity - 30 Bus System

PMU / PDC	Optimal										Redundant		
	1	2	6	9	10	12	15	19	25	27	7	17	22
1		✓						✓			✓		
2	✓				✓				✓				
3				✓						✓			
4			✓			✓						✓	
5							✓						✓

as indicated in Tables 5.2, 5.3, and 5.4. Under a PDC attack, the compromised PDC is disconnected from the network to prevent attack propagation, which has an impact on the system observability as discussed before. To mitigate the impact of such attack, we re-route the uncompromised disconnected PMUs to other PDCs in the network using different approaches, and we comment on the observed outcome.

Single PDC Attack

In the first set of experiments, we disconnected PDC-2 along with the connected PMUs from the WAMS network of the bus systems under study. This resulted in a drop in system observability to 71%, 84% and 77% for 14-Bus, 24-Bus and 30-Bus systems respectively due to loss of PMU data stream from PDC-2. To mitigate this loss in observability, we executed the proposed model along with the approach presented in [89] and the observability-base model. Based on our approach, measurements from the disconnected PMUs are routed to new PDCs as shown in Table 5.5. The effect of this reestablished connectivity on system observability is presented in Table 5.6. As Table 5.6 shows, all approaches achieve 100% observability of the 14-Bus system while varying the timer value for the available PDCs. This is mainly due to the small system size which allows the timely arrival of the rerouted measurements from the disconnected PMUs to the newly assigned PDCs, and thus full system observability.

The increase in system size, as in the case of 24-Bus and 30-Bus systems, affects the

achieved observability. This effect can be best noticed for the base approach which aims at achieving observability without any consideration of the network status. The increase in system size affects the observability achieved by [89] in the presence of a short PDC timer period (30 ms) since the approach presented in [89] considers end-to-end network delay without any consideration for the PDC times restrictions. Compared to the previous approaches, our proposed model succeeds in attaining a 100% system observability for various timer values since it considers this factor among others while rerouting the measurements from the disconnected PDC.

Table 5.5: Optimal PMU to PDC Post Attack Connectivity

Test System	Single PDC Attack		Multiple PDC Attack	
	PMU	PDC	PMU	PDC
14-Bus	6	3	*	1
24-Bus	2	1	2	1
	8	3	8	4
			10	1
			23	1
30-Bus	1	5	1	3
	10	5	10	5
	25	3	25	3
			6	5
			12	5

Multiple PDC Attack

For the second set of experiments, we consider an attack on multiple PDCs in the WAMS network. Along with PDC-2 that fails in the first set of experiments, PDC-3 and PDC-4 are disconnected from the 24-Bus and 30-Bus networks respectively, and can no longer forward PMU data streams. Due to loss of those PDCs, system observability drops

Table 5.6: Observability percentage under single PDC attack

Test System	Model	Timer			
		30 ms	40 ms	50 ms	60 ms
IEEE 14-Bus	Proposed Model	100%	100%	100%	100%
	Lin. et. al. [89]	100%	100%	100%	100%
	Observability	100%	100%	100%	100%
IEEE 24-Bus	Proposed Model	100 %	100%	100%	100%
	Lin. et. al. [89]	92%	100%	100 %	100 %
	Observability	46 %	63%	63 %	71 %
IEEE 30-Bus	Proposed Model	100 %	100 %	100 %	100 %
	Lin. et. al. [89]	92 %	100 %	100 %	100 %
	Observability	87 %	90 %	90 %	90 %

to 57%, 62%, and 53% for 14-Bus, 24-Bus, and 30-Bus systems respectively. Following a similar approach to that in the presence of a single PDC failure, we attempted to improve the system observability through routing of disconnected PMUs to the available PDCs using different approaches. For post attack recovery, our proposed model connects the disconnected PMUs to available PDCs as outlined in Table 5.5. This allows for the collection of measurements from those PMUs, and the reevaluation of system observability. The effect of this connectivity on observability is presented in Table 5.7. The collected results demonstrate the ability of our proposed approach to ensure 100% system observability for the 14-Bus system for different PDC timer values, while the other two approaches fail in ensuring full system observability for short PDC timer values. This loss in observability is mainly caused by the need to reroute more measurements over communication channels that were already in use. This change results in an increase in the communication delay over those links, and thus PMU measurements arrival upon expiration of PDC timer. Moreover, for the 24-Bus system, the proposed approach outperforms the other two for strict timer requirements (30 ms) and achieves complete system observability for larger timer values.

Table 5.7: Observability percentage under multiple PDC attack

Test System	Model	Timer			
		30 ms	40 ms	50 ms	60 ms
IEEE 14-Bus	Proposed Model	100%	100%	100%	100%
	Lin. et. al. [89]	71%	100%	100%	100%
	Observability	64 %	64 %	64 %	64 %
IEEE 24-Bus	Proposed Model	92 %	100 %	100 %	100 %
	Lin. et. al. [89]	87 %	100 %	100 %	100 %
	Observability	25 %	87 %	83 %	55 %
IEEE 30-Bus	Proposed Model	100 %	100 %	100 %	100 %
	Lin. et. al. [89]	92 %	100 %	100 %	100 %
	Observability	30 %	30 %	40 %	57 %

However, the observability-base model suffers most due to the large changes in the system and the need to reroute several measurements. This leads to dropping various needed measurements that do not make it before the timer expiration of receiving PDCs. As for the 30-Bus system, our model outperforms the other approaches and succeeds in achieving 100% observability for all timer values. The observability-based approach suffers most the effects of increase in network size and drop in number of available PDCs.

5.3.2 WAMS network with redundant PMUs:

In this section, we randomly introduce additional PMUs to the WAMS network. We add two PMUs for the 14-Bus system, and three PMUs for each of the 24-Bus and 30-Bus systems. The bus locations of those PMUs and the PDCs they are connected to are indicated in Tables 5.2, 5.3, and 5.4. This allows us to evaluate the success of the different approaches in attaining post PDC attack system observability for the cases of attack on single or multiple PDCs in the presence of redundant PMU measurements.

Table 5.8: System Observability in presence of redundant PMUs and attack on single PDC

Test System	Model	Timer			
		30 ms	40 ms	50 ms	60 ms
IEEE 14-bus	Proposed Model	100%	100%	100%	100%
	Lin. et. al. [89]	100%	100%	100%	100%
	Observability	93%	93%	86%	100%
IEEE 24-bus	Proposed Model	100 %	100 %	100 %	100 %
	Lin. et. al. [89]	100 %	100 %	100 %	100 %
	Observability	58 %	87 %	100 %	100 %
IEEE 30-bus	Proposed Model	100 %	100 %	100 %	100%
	Lin. et. al. [89]	100%	100%	100%	100 %
	Observability	93 %	80 %	93 %	80 %

Single PDC Attack

We again consider an attack that results in the disconnection of PDC-2 from the WAMS network. In the presence of redundant PMUs, system observability achieved by the different approaches is outlined in Table 5.8.

Similar to the setup in Section 5.3.1, we evaluated the different approaches while varying the timer for the available PDCs. As can be noticed from the results in Table 5.8, the availability of redundant PMUs has a negative impact on the achieved observability using the base method in the case of 14-Bus systems. This is mainly due to the delay imposed by the redundant measurements on the communication network, and resulting in the arrival of optimal PMU measurements upon PDC timer expiration. However, for our approach and that of [89], the availability of redundant measurements does not impact system observability since both approaches consider the network delay when rerouting disconnected PMU measurements to available PDCs.

Multiple PDC Attack

In the presence of an attack targeting multiple PDCs, more PMUs are disconnected and thus there is a need to reestablish connectivity between these PMUs and the available PDCs. The success of the different approaches in establishing this connectivity and improving post attack system observability is presented in Table 5.10. For the IEEE 14-Bus system, the proposed approach succeeds in restoring full system observability for different PDC timer values. This gives an advantage for our solution over the base approach and that of [89]. This advantage is a result of considering an additional factor when reestablishing the connectivity, namely the restrictions imposed by the PDC timer values. This advantage is more noticeable with the increase in the system size as is the case with the 24-Bus and 30-Bus systems, where the proposed model outperforms the other approaches in the achieved system observability. However, comparing those results with the ones from Table 5.7, we can notice that the availability of additional PMUs is not sufficient to get better observability. The lack of positive impact of redundant PMUs on post attack observability can be understood as a result of the alteration in network traffic and PDC timer functionality, where redundant measurements might be first arrivals at a PDC and trigger the respective PDC timer. Thus, not providing a large enough window for needed measurements to arrive at their destination PDCs in a timely manner.

Table 5.9: Redundant PMU-PDC Post Attack Connectivity

Test System	Single PDC Attack		Multiple PDC Attack	
	PMU	PDC	PMU	PDC
14-Bus	6	3	*	1
24-Bus	2	1	2	1
	8	1	8	4
			10	1
			23	1
30-Bus	1	5	1	1
	10	-	10	5
	25	3	25	3
			6	1
			12	5
			17	-

Table 5.10: System Observability in presence of redundant PMUs and attack on multiple PDCs

Test System	Model	Timer			
		30 ms	40 ms	50 ms	60 ms
IEEE 14-bus	Proposed Model	100%	100%	100%	100%
	Lin. et. al. [89]	50%	64%	100%	100%
	Observability	79%	36%	86%	72%
IEEE 24-bus	Proposed Model	96 %	92 %	100 %	100 %
	Lin. et. al. [89]	84 %	75 %	100 %	100 %
	Observability	54 %	50 %	50 %	62 %
IEEE 30-bus	Proposed Model	100 %	100%	100 %	100 %
	Lin. et. al. [89]	80 %	100 %	100 %	100 %
	Observability	80 %	70 %	70 %	70 %

6. Conclusion

6.1 Summary

This thesis addressed several challenges and concerns associated with WAMS communication network security. Mainly, it focused on the relation between WAMS security and the IP routing protocol, which is an essential aspect of the collection of synchrophasor measurements.

At first, Chapter 2 presented an overview of WAMS, its benefits, components, and security concerns. We concluded Chapter 2 with a survey of the existing literature work addressing attacks targeting WAMS and the impact of such attacks on the operations of the grid.

Motivated by the challenges learned from the literature survey, in chapter 3, we proposed a mathematical model for PMU communication routing in WAMS to enhance the network performance against delay attacks. The objective of this model is minimize the number of invalid measurements, which are measurements that arrive after the expiration of the PDC timer or after the end-to-end delay threshold. We considered different IEEE test systems to evaluate the performance of our proposed model in comparison with different approaches. Then, we simulated a delay attack targeting critical links on the network. We observe that in case of an attack our proposed model manages to find trees that minimize the impact of delays while satisfying real-time requirements.

Next, in chapter 4, we studied the propagation of cyber-attacks in WAMS. We addressed

the relation between cyber-attack propagation and IP multicast routing protocol in PMUs network. We presented a mathematical formulation of a multicast tree construction model that minimizes the probability of attack propagation while satisfying real time and capacity requirements. We evaluated our proposed multicast trees in comparison with shortest path multicast trees. Our numerical results show that our proposed tree model achieves lower probability of cyber-attack propagation even for larger test systems.

Synchrophasor technology is used for real-time control and monitoring in smart grid. The delivery of phasor measurements from PMUs to the control center relies on the availability of a reliable communication network, and phasor data concentrators to align and aggregate measurements into data streams. The loss of a PDC from this network affects a stream of phasors from several PMUs. Thus, recovery from PDC failure or loss is essential for the timely delivery of phasor measurements to control and monitoring applications. Therefore, in chapter 5, we proposed a post PDC failure recovery scheme to restore connectivity with disconnected PMUs, and recover thier phasor measurements. The proposed scheme is mathematically formulated into a linear program that considers the functional details of the WAMS network, and succeeds in reestablishing the affected system observability. Tests on the IEEE standard bus systems demonstrated the usability and effectiveness of our approach in maintaining system observability, and its advantage over other approaches in the literature.

6.2 Future Directions

Over the past two decades, the research community has witnessed a wave of discussion toward setting the path for the grid of the future, a smart, failure and attack-resilient, and self-healing grid. We have witnessed the birth of advanced technologies and applications that enable the migration towards the smart grid. Those applications and technologies are introducing new vulnerabilities to cyber-attacks. In this thesis, we have addressed several

challenges associated with the security of WAMS. This section of the thesis highlights potential challenges and directions for future research.

6.2.1 Effective Delay Attack

As mentioned previously, WAMS applications rely on synchrophasor from remote measurement devices at substations and in the field. synchrophasor measurements are communicated back to the control center/application using a variety of protocols and communication media such as the IEEE C37.118 and the IEC 61850-90-5. The remote sensors and the communication channels over which their readings are communicated present an attack surface for attackers wanting to disrupt power system operations. Even though WAMS communication network tends to be a dedicated Intranet, this does not mean that such networks are immune to cyber-attacks. In general, integrity attack such as false data injection has been extensively studied in the literature and methods to choose the best attack vector to cause an impact on the system without being detected has been proposed. Compared to integrity attack, availability attack is considered easier since it requires fewer resources to launch the attack. However, having a simple arbitrary delay attack might not have an impact on the grid operations. Therefore, a straightforward availability attack might not achieve the attacker objectives to disturb the grid operation. This is due to the fact that simply choosing random links to attack is not sufficient and the attacker needs to select critical links carefully. Moreover, the amount of delay to inject in the network without being detected need to be studied. Finally, the attacker needs to have a good understanding of the communication network on hand to launch a successful availability attack. With the aforementioned challenges in mind, an attacker model to find critical links to attack and how much delay to inject in the network to disturb the grid operation without being detected is a potential future work that needs to be investigated.

In particular, WAMS applications can be significantly affected by an availability attack

since it heavily depends on transmitted synchrophasor. Therefore, the attacker should introduce a network delay such that some measurements arrive after the expiration of the PDC timer and then will be dropped at the PDC. The objective of the attacker should be to find the minimum number of links to attack to cause a drop of measurements at the PDC (due to the expiration of the timer) and have an impact on the application without being detected. Moreover, the attacker needs to find the amount of delay to inject such that measurements are being dropped at the PDC without being detected.

6.2.2 Delay Attack and Its Impact on Voltage Stability

Another possible future work direction is understanding delay attack and its impact on voltage stability. Voltage stability has been regarded as one of the primary threats to the security of modern power network operation during the past few decades. Power system disturbances such as a continuous load increase and/or a major change in network topology can result in voltage collapse. To avoid voltage collapse in a stressed power system, adequate VAR support, which aims to maintain system voltage and to reduce real power transmission loss, is required. Indeed, reactive power can be dispatched effectively to achieve a secure and economic grid operation. A number of planning and operation technologies have been proposed to reduce the possibility of voltage collapse.

Voltage regulation is important for maintaining the quality of power measured by the voltage levels at the consumers' side, which must stay within a given admissible range at all times. One of the critical devices used for this control is the load ration control transformers (LRTs) located at distribution substations. These are transformers whose secondary voltage can be varied through switching their taps. Conventional control is based on the so-called line drop compensator (LDC), which estimates the voltage at a fixed remote point in the network via local measurements at the substation. However, when distributed generators

are connected, steady state voltage rise may occur within the feeder. This changes the profile characteristics, severely limiting the applicability of LDC. One solution to this issue is to use sectionizing switches with sensors (called IT switches) in the feeders. Such switches may be equipped with sensors for phase voltages and currents and also have voltage and current transformers. By connecting the switches to the voltage regulator they can send their voltage measurements. The voltage regulator can then obtain a more accurate voltage profile of the feeder in real time to help determine the necessary output voltage level and thus the tap position there. Notice that the use of voltage measurements in the grid requires real-time data communication of the measurements from the switches. This increases the chances of data delay and falsification by malicious attackers. The attacker may falsify or delay a number of sensor measurement data to cause irregular tap changes, which may result in voltage violation at feeder nodes or unnecessary tap changes that can damage the device.

A demonstration of the impact of delay attack on the voltage stability through the use of a simulator such as GridLAB-D, a power distribution system simulation and analysis tool, to show the impact of unnecessary tap changes on the voltage stability is an interesting point to be investigated.

After that, a mitigation mechanism to mitigate the impact of delay attacks need to be studied. This mechanism will leverage the fact that the voltage profile in the feeder becomes a decreasing function of distance from the substation. Hence, the estimate of the delayed measurements can be made based on the voltage and the current at the LRT, the topology information, past load data, and so on.

6.2.3 Robust PMU-PDC connectivity against loss of PDCs

Finally, as mentioned in 5, the disconnection of some PDCs due to cyber-attacks has an impact on the system observability. However, it is possible to reconnect some disconnected

yet uncompromised PMUs to the communication network to restore the system observability. During the process of reconnecting un-compromised PMUs, the timer of each PDC and the end-to-end delay need to be considered. Moreover, this reconnecting process should not have an impact on other connected PMUs into consideration. As a continuation for this work, an approach to design WAMS network robust against PDC loss can be investigated. Such an approach should consider initial PMU to PDC connectivity that ensures the timely collection of phasor measurements in the absence and presence of cyber attacks that might bring one or several PDCs out of service.

Bibliography

[1] NIST Framework. Roadmap for Smart Grid Interoperability Standards. *NIST special publication*, 1108, 2010.

[2] György Dán, H. Sandberg, Mathias Ekstedt, and Gunnar Björkman. Challenges in power system information security. *Security Privacy, IEEE*, 10(4):62–70, July 2012.

[3] US DOE Electricity Delivery. Synchrophasor technologies and their deployment in the recovery act smart grid programs, 2013.

[4] Ieee guide for phasor data concentrator requirements for power system protection, control, andmonitoring. *IEEE Std C37.244-2013*, pages 1–65, May 2013.

[5] Andersson. et.al. Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. *Power Systems, IEEE Transactions on*, 20(4), 2005.

[6] U.S.-Canada Power System Outage Task Force. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Technical report, 04 2004.

[7] US DoE. The smart grid: An introduction, 2008.

[8] Xu Li, Xiaohui Liang, Rongxing Lu, Xuemin Shen, Xiaodong Lin, and Haojin Zhu. Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine*, 50(8), 2012.

[9] V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G.P. Hancke. Smart grid technologies: Communication technologies and standards. *Industrial Informatics, IEEE Transactions on*, 7(4):529–539, Nov 2011.

[10] Patrick McDaniel and Stephen McLaughlin. Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, 7(3):75–77, 2009.

[11] Paul T Myrda, Jeffrey Taft, and Paul Donner. Recommended approach to a naspinet architecture. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 2072–2081. IEEE, 2012.

[12] Ragib Hasan, Rakesh Bobba, and Himanshu Khurana. Analyzing naspinet data flows. In *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES*, pages 1–6. IEEE, 2009.

[13] Seyedbehzad Nabavi, Jianhua Zhang, and Aranya Chakrabortty. Distributed optimization algorithms for wide-area oscillation monitoring in power systems using interregional pmu-pdc architectures. *IEEE Transactions on Smart Grid*, 6(5):2529–2538, 2015.

[14] Soummya Kar and Gabriela Hug. Distributed robust economic dispatch in power systems: A consensus+ innovations approach. In *Power and Energy Society General Meeting, 2012 IEEE*, pages 1–8. IEEE, 2012.

[15] Ziang Zhang and Mo-Yuen Chow. Convergence analysis of the incremental cost consensus algorithm under different communication network topologies in a smart grid. *Power Systems, IEEE Transactions on*, 27(4):1761–1768, 2012.

[16] Emiliano Dall'Anese, Hao Zhu, and Georgios Giannakis. Distributed optimal power flow for smart microgrids. *Smart Grid, IEEE Transactions on*, 4(3):1464–1475, 2013.

[17] Tomaso Erseghe. Distributed optimal power flow using admm. *Power Systems, IEEE Transactions on*, 29(5):2370–2380, 2014.

[18] OPNET Simulator. `http://www.riverbed.com/products/performance-management-control/opnet.html`. Last accessed on: 04-02-2015.

[19] HYPERSIM, Real-Time Digital Power System Simulator. `http://www.hydroquebec.com/innovation/en/pdf/2010G080-16A-Hypersim.pdf`. Last accessed on: 04-02-2015.

[20] Dongchan Lee and Deepa Kundur. Cyber attack detection in pmu measurements via the expectation-maximization algorithm. In *Signal and Information Processing (GlobalSIP), 2014 IEEE Global Conference on*, pages 223–227. IEEE, 2014.

[21] Hua Lin, Yi Deng, Sandeep Shukla, James Thorp, and Lamine Mili. Cyber security impacts on all-pmu state estimator-a case study on co-simulation platform geco. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 587–592. IEEE, 2012.

[22] Anthony R Metke and Randy L Ekl. Smart grid security technology. In *Innovative Smart Grid Technologies (ISGT), 2010*, pages 1–7. IEEE, 2010.

[23] Rakesh B Bobba, Katherine M Rogers, Qiyan Wang, Himanshu Khurana, Klara Nahrstedt, and Thomas J Overbye. Detecting false data injection attacks on dc state estimation. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, volume 2010, 2010.

[24] Tung T Kim and H Vincent Poor. Strategic protection against data injection attacks on power grids. *IEEE Transactions on Smart Grid*, 2(2):326–333, 2011.

[25] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. Malicious data attacks on the smart grid. *Smart Grid, IEEE Transactions on*, 2(4):645–658, 2011.

[26] Rakesh B Bobba, Jeff Dagle, Erich Heine, Himanshu Khurana, William H Sanders, Peter Sauer, and Tim Yardley. Enhancing grid measurements: Wide area measurement systems, naspinet, and security. *Power and Energy Magazine, IEEE*, 10(1):67–73, 2012.

[27] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, pages 800–82, 2011.

[28] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13, 2011.

[29] André Teixeira, György Dán, Henrik Sandberg, and Karl H Johansson. A cyber security study of a scada energy management system: Stealthy deception attacks on the state estimator. *arXiv preprint arXiv:1011.1828*, 2010.

[30] Kun Zhu, Ahmad T Al-Hammouri, and Lars Nordström. To concentrate or not to concentrate: Performance analysis of ict system with data concentrations for wide-area monitoring and control systems. In *Power and Energy Society General Meeting, 2012 IEEE*, pages 1–7. IEEE, 2012.

[31] Anjan Bose. Smart transmission grid applications and their supporting infrastructure. *IEEE Transactions on Smart Grid*, 1(1):11–19, 2010.

[32] Yufeng Xin and Aranya Chakrabortty. A study on group communication in distributed wide-area measurement system networks in large power systems. In *Global*

Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE, pages 543–546. IEEE, 2013.

[33] Kun Zhu, Moustafa Chenine, Lars Nordstrom, Sture Holmstrom, and Goran Ericsson. Design requirements of wide-area damping systems—using empirical data from a utility ip network. *IEEE Transactions on Smart Grid*, 5(2):829–838, 2014.

[34] Shaobu Wang, Wenzhong Gao, Jianhui Wang, and Jin Lin. Synchronized sampling technology-based compensation for network effects in wams communication. *IEEE Transactions on Smart Grid*, 3(2):837–845, 2012.

[35] North American Syncro-Phasor Initative Network. Phasor gateway technical spesification for north american syncro-phasor initiative network (naspinet). 2009.

[36] Yi Deng. et.al. Communication network modeling and simulation for wide area measurement applications. In *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, Jan 2012.

[37] Seyedamirabbas Mousavian, Jorge Valenzuela, and Jianhui Wang. A probabilistic risk mitigation model for cyber-attacks to pmu networks. *Power Systems, IEEE Transactions on*, 30(1):156–165, 2015.

[38] Maik Seewald. Building an architecture based on ip-multicast for large phasor measurement unit (pmu) networks. In *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, pages 1–5. IEEE, 2013.

[39] NASPI Data and Network Systems Group Network Management Task Team. NASPI 2014 Survey of Synchrophasor System Networks – Results and Findings. Technical report, 07 2015.

[40] P. Donner and N. Yadav. Controlled distribution of phasor measurement data using multicast routing, July 15 2014. US Patent 8,780,706.

[41] M Kanabar, MG Adamiak, and J Rodrigues. Optimizing wide area measurement system architectures with advancements in phasor data concentrators (pdcs). In *Power and energy society general meeting (PES), 2013 IEEE*, pages 1–5. IEEE, 2013.

[42] Mark Adamiak, Bogdan Kasztenny, and William Premerlani. Synchrophasors: definition, measurement, and application. *Proceedings of the 59th Annual Georgia Tech Protective Relaying, Atlanta, GA*, pages 27–29, 2005.

[43] Suzhi Bi and Ying Jun Zhang. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Transactions on Smart Grid*, 5(3):1216–1227, 2014.

[44] M.A Rahman, E. Al-Shaer, and M.A Rahman. A formal model for verifying stealthy attacks on state estimation in power grids. In *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pages 414–419, Oct 2013.

[45] Deepjyoti Deka, Ross Baldick, and Sriram Vishwanath. Optimal hidden scada attacks on power grid: A graph theoretic approach. In *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pages 36–40. IEEE, 2014.

[46] Suzhi Bi and Ying Jun Zhang. Using covert topological information for defense against malicious attacks on dc state estimation. *IEEE Journal on Selected Areas in Communications*, 32(7):1471–1485, 2014.

[47] Md Ashfaqur Rahman and Hamed Mohsenian-Rad. False data injection attacks with incomplete information against smart power grids. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 3153–3158. IEEE, 2012.

[48] Jinsub Kim, Lang Tong, and Robert J Thomas. Subspace methods for data attack on state estimation: A data driven approach. *arXiv preprint arXiv:1406.0866*, 2014.

[49] Gabriela Hug and Joseph A Giampapa. Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks. *Smart Grid, IEEE Transactions on*, 3(3):1362–1370, 2012.

[50] Md Ashfaqur Rahman and Hamed Mohsenian-Rad. False data injection attacks against nonlinear state estimation in smart power grids. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, pages 1–5. IEEE, 2013.

[51] Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, and Wei Zhao. On false data-injection attacks against power system state estimation: Modeling and countermeasures. *Parallel and Distributed Systems, IEEE Transactions on*, 25(3):717–729, 2014.

[52] Suzhi Bi and Ying Jun Angela Zhang. Defending mechanisms against false-data injection attacks in the power system state estimation. In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pages 1162–1167. IEEE, 2011.

[53] Annarita Giani, Eilyan Bitar, Manuel Garcia, Miles McQueen, Pramod Khargonekar, and Kameshwar Poolla. Smart grid data integrity attacks. *Smart Grid, IEEE Transactions on*, 4(3):1244–1253, 2013.

[54] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 220–225. IEEE, 2010.

[55] Kate L Morrow, Erich Heine, Katherine M Rogers, Rakesh B Bobba, and Thomas J Overbye. Topology perturbation for detecting malicious data injection. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 2104–2113. IEEE, 2012.

[56] Suzhi Bi and Ying Jun Zhang. Mitigating false-data injection attacks on dc state estimation using covert topological information. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 766–771. IEEE, 2013.

[57] Suzhi Bi and Ying Jun Zhang. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Trans. Smart Grid*, pages 1216–1227, 2014.

[58] Mohammad Esmalifalak, Nam Tuan Nguyen, Rong Zheng, and Zhu Han. Detecting stealthy false data injection using machine learning in smart grid. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 808–813. IEEE, 2013.

[59] Lanchao Liu, Mohammad Esmalifalak, and Zhu Han. Detection of false data injection in power grid exploiting low rank and sparsity. In *Communications (ICC), 2013 IEEE International Conference on*, pages 4461–4465. IEEE, 2013.

[60] Lanchao Liu, M. Esmalifalak, Qifeng Ding, V.A Emesih, and Zhu Han. Detecting false data injection attacks on power grid by sparse optimization. *Smart Grid, IEEE Transactions on*, 5(2):612–621, March 2014.

[61] Yun Gu, Ting Liu, Dai Wang, Xiaohong Guan, and Zhanbo Xu. Bad data detection method for smart grids based on distributed state estimation. In *Communications (ICC), 2013 IEEE International Conference on*, pages 4483–4487, June 2013.

[62] Ting Liu, Yun Gu, Dai Wang, Yuhong Gui, and Xiaohong Guan. A novel method to detect bad data injection attack in smart grid. In *INFOCOM'13*, pages 3423–3428, 2013.

[63] Hanie Sedghi and Edmond Jonckheere. Statistical structure learning of smart grid for detection of false data injection. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, pages 1–5. IEEE, 2013.

[64] Saranya Parthasarathy and Deepa Kundur. Bloom filter based intrusion detection for smart grid scada. In *Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on*, pages 1–6. IEEE, 2012.

[65] Jorge Valenzuela, Jianhui Wang, and Nancy Bissinger. Real-time intrusion detection in power system operations. *Power Systems, IEEE Transactions on*, 28(2):1052–1062, 2013.

[66] Rob Mitchell and Ray Chen. Behavior-rule based intrusion detection systems for safety critical smart grid applications. *Smart Grid, IEEE Transactions on*, 4(3):1254–1263, 2013.

[67] Hyojun Lim and Chongkwon Kim. Multicast tree construction and flooding in wireless ad hoc networks. In *Proceedings of the 3rd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, pages 61–68. ACM, 2000.

[68] S Ramanathan. Multicast tree generation in networks with asymmetric links. *IEEE/ACM transactions on Networking*, 4(4):558–568, 1996.

[69] George N. Rouskas and Ilia Baldine. Multicast routing with end-to-end delay and delay variation constraints. *IEEE Journal on Selected Areas in communications*, 15(3):346–356, 1997.

[70] Qing Zhu, Mehrdad Parsa, and JJ Garcia-Luna-Aceves. A source-based algorithm for delay-constrained minimum-cost multicasting. In *INFOCOM'95. Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Bringing Information to People. Proceedings. IEEE*, volume 1, pages 377–385. IEEE, 1995.

[71] Hussein F Salama, Douglas S Reeves, and Yannis Viniotis. Evaluation of multicast routing algorithms for real-time communication on high-speed networks. *IEEE Journal on Selected Areas in Communications*, 15(3):332–345, 1997.

[72] Husheng Li, Lifeng Lai, and H Vincent Poor. Multicast routing for decentralized control of cyber physical systems with an application in smart grid. *IEEE Journal on Selected Areas in Communications*, 30(6):1097–1107, 2012.

[73] Quanyan Zhu, Dong Wei, and Tamer Basar. Secure routing in smart grids. In *Workshop on Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS)*, pages 55–59, 2011.

[74] Ronghui Hou, Chuqing Wang, Quanyan Zhu, and Jiandong Li. Interference-aware qos multicast routing for smart grid. *Ad Hoc Networks*, 22:13–26, 2014.

[75] Jin Wei and Deepa Kundur. Goalie: goal-seeking obstacle and collision evasion for resilient multicast routing in smart grid. *IEEE Transactions on Smart Grid*, 7(2):567–579, 2016.

[76] Xichen Jiang, Jiangmeng Zhang, Brian J Harding, Jonathan J Makela, Alejandro D Domı, et al. Spoofing gps receiver clock offset of phasor measurement units. *IEEE Transactions on Power Systems*, 28(3):3253–3262, 2013.

[77] Daniel P Shepard, Todd E Humphreys, and Aaron A Fansler. Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3-4):146–153, 2012.

[78] Moustafa Chenine and Lars Nordström. Investigation of communication delays and data incompleteness in multi-pmu wide area monitoring and control systems. In *Electric Power and Energy Conversion Systems, 2009. EPECS'09. International Conference on*, pages 1–6. IEEE, 2009.

[79] Moustafa Chenine and Lars Nordstrom. Modeling and simulation of wide-area communication for centralized pmu-based applications. *IEEE Transactions on Power Delivery*, 26(3):1372–1380, 2011.

[80] Hua Lin, Yi Deng, Sandeep Shukla, James Thorp, and Lamine Mili. Cyber security impacts on all-pmu state estimator-a case study on co-simulation platform geco. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 587–592. IEEE, 2012.

[81] Chuan-Ke Zhang, Lin Jiang, QH Wu, Yong He, and Min Wu. Delay-dependent robust load frequency control for time delay power systems. *IEEE Transactions on Power Systems*, 28(3):2192–2201, 2013.

[82] Arman Sargolzaei, Kang Yen, and MN Abdelghani. Delayed inputs attack on load frequency control in smart grid. In *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, pages 1–5. IEEE, 2014.

[83] Martin Lévesque and David Tipper. A survey of clock synchronization over packet-switched networks. *IEEE Communications Surveys & Tutorials*, 18(4):2926–2947, 2016.

[84] Yin Hong Chang, Panida Jirutitijaroen, and Chee-Wooi Ten. A simulation model of cyber threats for energy metering devices in a secondary distribution network. In *Critical Infrastructure (CRIS), 2010 5th International Conference on*, pages 1–7. IEEE, 2010.

[85] Mine Altunay, Sven Leyffer, Jeffrey T Linderoth, and Zhen Xie. Optimal response to attacks on the open science grid. *Computer Networks*, 55(1):61–73, 2011.

[86] Stanislav Ponomarev and Travis Atkison. Industrial control system network intrusion detection by telemetry analysis. *IEEE Transactions on Dependable and Secure Computing*, 13(2):252–260, 2016.

[87] Chee-Wooi Ten, Govindarasu Manimaran, and Chen-Ching Liu. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 40(4):853–865, 2010.

[88] Ahmad F Taha, Junjian Qi, Jianhui Wang, and Jitesh H Panchal. Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. *IEEE Transactions on Smart Grid*, 2016.

[89] Hui Lin, Chen Chen, Jianhui Wang, Junjian Qi, Dong Jin, Zbigniew Kalbarczyk, and Ravishankar K Iyer. Self-healing attack-resilient pmu network for power system operation. *IEEE Transactions on Smart Grid*, 2016.

[90] Arbiter systems power sentinel denial-of-service vulnerabilities. `https://ics-cert.us-cert.gov/advisories/ICSA-12-249-01`. Accessed: May 2015.

[91] National Instruments. What is the ni grid automation system?, 2015.

[92] Yichi Zhang, Lingfeng Wang, and Weiqing Sun. Trust system design optimization in smart grid network infrastructure. *IEEE Transactions on Smart Grid*, 4(1):184–195, 2013.

[93] Arman Sargolzaei, Kang K Yen, and Mohamed N Abdelghani. Preventing time-delay switch attack on load frequency control in distributed power systems. *IEEE Transactions on Smart Grid*, 7(2):1176–1185, 2016.

[94] Kun Zhu, Moustafa Chenine, and Lars Nordstrom. Ict architecture impact on wide area monitoring and control systems' reliability. *IEEE transactions on power delivery*, 26(4):2801–2808, 2011.

[95] Daniel Dotta, Aguinaldo S e Silva, and Ildemar C Decker. Wide-area measurements-based two-level control design considering signal transmission delay. *IEEE Transactions on Power Systems*, 24(1):208–216, 2009.

[96] Hongxia Wu, Hui Ni, and GT Heydt. The impact of time delay on robust control design in power systems. In *Power Engineering Society Winter Meeting, 2002. IEEE*, volume 2, pages 1511–1516. IEEE, 2002.

[97] Can Huang, Fangxing Li, Tao Ding, Yuming Jiang, Jiahui Guo, and Yilu Liu. A bounded model of the communication delay for system integrity protection schemes. *IEEE Transactions on Power Delivery*, 31(4):1921–1933, 2016.

[98] Yang Wang, Wenyuan Li, and Jiping Lu. Reliability analysis of wide-area measurement system. *IEEE Transactions on Power Delivery*, 25(3):1483–1491, 2010.

[99] Fang Zhang, Yuanzhang Sun, Lin Cheng, Xiong Li, Joe H Chow, and Weixing Zhao. Measurement and modeling of delays in wide-area closed-loop control systems. *IEEE Transactions on Power Systems*, 30(5):2426–2433, 2015.

[100] Chao Lu, Xinran Zhang, Xiaoyu Wang, and Yingduo Han. Mathematical expectation modeling of wide-area controlled power systems with stochastic time delay. *IEEE Transactions on Smart Grid*, 6(3):1511–1519, 2015.

[101] Mitalkumar G Kanabar, Tarlochan S Sidhu, and Mohammad RD Zadeh. Laboratory investigation of iec 61850-9-2-based busbar and distance relaying with corrective measure for sampled value loss/delay. *IEEE Transactions on Power Delivery*, 26(4):2587–2595, 2011.

[102] Prashant Kansal and Anjan Bose. Bandwidth and latency requirements for smart transmission grid applications. *IEEE Transactions on Smart Grid*, 3(3):1344–1352, 2012.

[103] Edsger W Dijkstra. A note on two problems in connexion with graphs. *Numerische mathematik*, 1(1):269–271, 1959.

[104] Ali Abur and Antonio Gomez Exposito. *Power system state estimation: theory and implementation*. CRC press, 2004.

[105] Saikat Chakrabarti and Elias Kyriakides. Optimal placement of phasor measurement units for power system observability. *IEEE Transactions on power systems*, 23(3):1433–1440, 2008.

[106] Beibei Li, Rongxing Lu, Wei Wang, and Kim-Kwang Raymond Choo. Ddoa: A dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system. *IEEE Transactions on Information Forensics and Security*, 11(11):2415–2425, 2016.

[107] Haris M Khalid and Jimmy C-H Peng. A bayesian algorithm to enhance the resilience of wams applications against cyber attacks. *IEEE Transactions on Smart Grid*, 7(4):2026–2037, 2016.

[108] Yiming Wu, Lars Nordström, and David E Bakken. Effects of bursty event traffic on synchrophasor delays in ieee c37. 118, iec61850, and iec60870. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pages 478–484. IEEE, 2015.

[109] Vijay K Sood, Daniel Fischer, JM Eklund, and Tim Brown. Developing a communication infrastructure for the smart grid. In *Electrical Power & Energy Conference (EPEC), 2009 IEEE*, pages 1–7. IEEE, 2009.

[110] Young-Jin Kim, Marina Thottan, Vladimir Kolesnikov, and Wonsuck Lee. A secure decentralized data-centric information infrastructure for smart grid. *IEEE Communications Magazine*, 48(11), 2010.

[111] Networking the smart grid. Tropos Wireless Commun. Syst., Sunnyvale, CA, USA, Sep 2010.

[112] US DOE. Communications requirements of smart grid technologies. *US Department of Energy, Tech. Rep*, pages 1–69, 2010.

[113] Mohamed Daoud, Xavier Fernando, et al. On the communication requirements for the smart grid. *Energy and Power Engineering*, 3(01):53, 2011.

[114] Emilio Ancillotti, Raffaele Bruno, and Marco Conti. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Computer Communications*, 36(17):1665–1697, 2013.

[115] Opal-rt technologies.

[116] Power System Relaying Committee et al. Ieee standards for synchrophasor measurements for power systems-ieee std c37. 118.1-2011. *New York, USA*, 2011.

[117] Open source software for creating private and public clouds.

[118] Opal-rt technologies.

[119] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. On malicious data attacks on power system state estimation. In *Universities Power Engineering Conference (UPEC), 2010 45th International*, pages 1–6. IEEE, 2010.

[120] ICS-CERT. OSIsoft Multiple Vulnerabilities. Available at:`https://ics-cert.us-cert.gov/advisories/ICSA-13-225-02`. Last accessed on May 2015.

[121] Ting Liu, Xiaohong Guan, Qinghua Zheng, and Yu Qu. A new worm exploiting ipv6 and ipv4-ipv6 dual-stack networks: experiment, modeling, simulation, and defense. *IEEE network*, 23(5), 2009.

[122] Bo Sun, Guanhua Yan, Yang Xiao, and T Andrew Yang. Self-propagating mal-packets in wireless sensor networks: Dynamics and defense implications. *Ad Hoc Networks*, 7(8):1489–1500, 2009.

[123] Robert G Cole, Nam Phamdo, Moheeb A Rajab, and Andreas Terzis. Requirements on worm mitigation technologies in manets. In *Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation*, pages 207–214. IEEE Computer Society, 2005.

[124] U.S. DoE. NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses . Technical report, 2010.

[125] PMU Networking with IP Multicast. 2012.

[126] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.

[127] PM Subcommittee. Ieee reliability test system. *IEEE Transactions on Power Apparatus and Systems*, pages 2047–2054, 1979.

[128] R Christie. Power system test archive. *University of Washington*, 1999.

[129] Anantha Pai. *Energy function analysis for power system stability*. Springer Science & Business Media, 2012.

[130] Saikat Chakrabarti, Elias Kyriakides, and Demetrios G Eliades. Placement of synchronized measurements for power system observability. *IEEE Transactions on Power Delivery*, 24(1):12–19, 2009.

[131] Igor Ivankovic, Srdjan Skok, and Boris Avramovic. Transmission power system dynamic mathematical model based on synchronized measurements. In *PowerTech, 2017 IEEE Manchester*, pages 1–6. IEEE, 2017.

[132] Hyde M Merrill and Fred C Schweppe. Bad data suppression in power system static state estimation. *Power Apparatus and Systems, IEEE Transactions on*, (6):2718–2725, 1971.

[133] Peng Yang, Zhao Tan, Ami Wiesel, and Arye Nehora. Power system state estimation using pmus with imperfect synchronization. *Power Systems, IEEE Transactions on*, 28(4):4162–4172, 2013.

[134] RF Nuqui and Arun G Phadke. Hybrid linear state estimation utilizing synchronized phasor measurements. In *Power Tech, 2007 IEEE Lausanne*, pages 1665–1669. IEEE, 2007.

[135] VH Quintana, A Simoes-Costa, and A Mandel. Power system topological observability using a direct graph-theoretic approach. *Power Apparatus and Systems, IEEE Transactions on*, (3):617–626, 1982.

[136] Erwin Enrique Fetzer and PM Anderson. Observability in the state estimation of power systems. *Power Apparatus and Systems, IEEE Transactions on*, 94(6):1981–1988, 1975.

[137] Ali Abur and Fernando H Magnago. Optimal meter placement for maintaining observability during single branch outages. *Power Systems, IEEE Transactions on*, 14(4):1273–1278, 1999.

[138] Ekram Hossain, Zhu Han, and H Vincent Poor. *Smart grid communications and networking*. Cambridge University Press, 2012.

[139] Bradley Stephenson and Biplab Sikdar. A quasi-species model for the propagation and containment of polymorphic worms. *IEEE Transactions on Computers*, 58(9):1289–1296, 2009.

[140] Peter Mell, Karen Kent, and Joseph Nusbaum. *Guide to malware incident prevention and handling*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2005.

[141] KE Martin, D Hamai, MG Adamiak, S Anderson, M Begovic, G Benmouyal, G Brunello, J Burger, JY Cai, B Dickerson, et al. Exploring the ieee standard c37. 118–2005 synchrophasors for power systems. *IEEE transactions on power delivery*, 23(4):1805–1811, 2008.

[142] Herbert Falk. Iec 61850–90–5 an overview. *Protection, Automation & Control World Magazine*, 2012.

[143] Reem Kateb, Parisa Akaber, Mosaddek Tushar, AL-Barakati Abdullah, Mourad Debbabi, and Chadi Assi. Enhancing wams communication network against delay attacks. *IEEE Transactions on Smart Grid*, 2018.